A. APPENDIX
ACRONYMS / GLOSSARY

AA	ASCII-to-ASCII (LMF)
AC	ASCII-to-Card (LMF)
ACK	Acknowledgment (Associated with data transfers)
ACP	Allied Communications Procedures
ADP	Automated Data Processing
AFAMPE	Air Force Automated Message Processing Equipment
AID	AUTODIN Interface Device
AIG	Address Indicator Group
AIS	Automated Information System
AMHS	Automated Message Handling System
AMME	Automated Multi-Media Exchange
AMPE	Automated Message Processing Equipment
AOI	Area of Interest
AOR	Area of Responsibility
API	Application Programming Interface
ASC	Automated Switching Center
ASCII	American Standard Code for Information Interchange
AT	ASCII-To-Tape
AUTODIN	Automatic Digital Network
AWIS	Army WWMCCS Information System
BCW	Block Control Word
BP	Block Parity
BPS	Bits Per Second
BSM	Basic Security Module
BSQ	Backside Queue
C2	Command and Control or Command Center
CA	Card-to-ASCII (LMF)
CAN	Cancel
CAP	Component Approval Process
CAU	Crypto Ancillary Unit
CBC	Comeback Copy
CBT	CSP Backside Terminal
CCPII	Communications Control Processor II
CCF	Classification Configuration File
CCU	Crypto Control Unit
CDF	Configuration Data File
CIC	Content Indicator Code
CINC	Commander-In-Chief
COE	Common Operating Environment
COMSEC	Communications Security
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRITIC	Critical Intelligence

CSD	Channel Sequence Designator
CSN	Channel Sequence Number
CT	Card-to-Tape (LMF)
CTS	Clear To Send
CWP	Code Word Protection
DB	Database
DAC	Discretionary Access Control
DART	Dynamic Analysis and Replanning Tool
daemon	A UNIX background task usually with no discernible user interface
DCA	Defense Communications Agency
DCAC	DCA Circular
DCE	Data Communications Equipment
DCS	Defense Communications System
DCT	Data Communications Terminal
DD173	Specific Joint Message Format enabling the message to be read by OCR
DEC	Digital Equipment Corporation
DISA	Defense Information Systems Agency
DLT	Data Line Terminal
DMS	Defense Message System
DOD	Department of Defense
DOI	DSSCS Operating Instructions
DOS	Disk Operating System
DPS	Data Processing System
DSRI	Destination Station Routing Indicator
DSSCS	Defense Special Security Communications System
DTE	Data Terminal Equipment
DTG	Date-Time-Group
E-MAIL	Electronic Mail
EAC	Emergency Action Cell
EDSS	EUCOM Decision Support System
EIA	Electronics Industry Association
EOF	End-Of-File
EOM	End-Of-Message Sentinel
EOR	End-Of-Routing
ETB	End-Of-Transmission Block
ETCC	European Theater Command Center
ETX	End-Of-Test Sentinel
EUCOM	European Command (same as USEUCOM)
FDDI	Fiber Distributed Data Interface
FEP	Front End Processor
FIFO	First-In-First-Out
FL	Format Line
FOC	Final Operating Capability
FTP	File Transfer Protocol
GCCS	Global Command and Control System
GB	Gigabyte
GENSER	General Services
GUI	Graphic User Interface
HI PRC	High Precedence
HQ	Headquarters

I/O	Input/Output
IAW	In Accordance With
IBM	International Business Machines
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
INV	Invalid Message
IOC	Initial Operating Capability
IP	Internet Protocol
JPEC	Joint Planning and Execution Community
JANAP	Joint Army Navy Air Force Publication
JMCIS	Joint Maritime Command Information System
JPL	Jet Propulsion Laboratory
KB	Kilobyte/Kilobaud
LCD	Liquid Crystal Display
LAN	Local Area Network
LDMX	Local Digital Message Exchange
LF	Line Feed
LIFO	Last In First Out (order)
LIMDIS	Limited Distribution (message routing)
LMF	Language Media Format
LTC	Line Terminal Controller
MAR	Message Action Record
MB	Megabyte
MDT	Mission Display System
MIL-STD	Military Standard
MM	Message Manager
MMAC	Multi-Media Access Center
MRA	Message Release Authority
MTF	Message Text Format
NAK	Negative Acknowledgment (Associated with Data Transfer)
NFS	Network File System
NITES	Navy Integrated Tactical Environment System
NOFORM	No Foreign
NOREP	No Reply
OCR	Optical Character Reader
OS	Operating System
OSRI	Originating Station Routing Indicator
OSS	Operational Support System
OSSN	Originating Station Sequence Number
P&P	Polling and Processing
PC	Personal Computer
PID	Process ID Number
PLA	Plain Language Address
PM	Preventive Maintenance
PROM	Programmable Read-Only Memory
R/T	Real-Time
PTC	Pentagon Telecommunications Center
raday	Message Processing Day
RAID	Redundant Array of Inexpensive Drives
RDBMS	Relational Database Management System

RAM	Random Access Memory
REP	Reply
RI	Routing Indicator
RICF	Routing Indicator Configuration File
RM	Reject Message
ROM	Read Only Memory
RTS	Request To Send
RxC	Receive Clock
RxD	Receive Data
SA	System Administration
SAT	Standard Automated Terminal
SCSI	Small Computer Systems Interface
SEL	Select Character
SIPRNET	Secret Internet Protocol Router Network
SMP	Section Message Processing
SOH	Start-Of-Header
SOM	Start-Of-Message
SOP	Standard Operating Procedure
SORTS	Status of Resources and Training System
SPECAT	Special Category (message routing)
SPECAT	Special Category Term
SSIC	Standard Subject Indicator Codes
SSN	Station Serial Number
SSO	System Security Officer
STACCS	Standard Theater Army Command and Control System
STX	Start-Of-Text
su	Super User
SYNC	Synchronous
TAI	Technology Applications Incorporated
TBS	To Be Supplied
TCC	Telecommunications Center
TFM	Trusted Facility Manual
TMA	Tasker and Message Assembler
TTI	Transitional Technology Incorporated
TxC	Transmit Clock
TxD	Transmit Data
UFS	UNIX File System
UPI	United Press International
USAWC	United States Army War College
USAFE	United States Air Force Europe
USMTF	US Message Text Format
VARDEF	Table of Variables
VDF	Verity Database
vi Session	A UNIX editing tool
WAN	Wide Area Network
WBT	Wait Before Transmitting
WIS	WWMCCS Information System
WWMCCS	Worldwide Military Command and Control System

B. APPENDIX - AMHS SERVER VER 3.1
INSTALLATION AND CONFIGURATION NOTES

Appendix B, "Installation and Configuration Notes," was provided by the U.S. Army (DISA) for inclusion in this publication. The OSF will distribute updates and/or additions to this Appendix periodically.

B.1 GCCS AMHS PREINSTALL PROCEEDURES

B.1.1 Minimum Hardware Requirements

SUN SPARC RUNNING SOLARIS 2.3 (at minimum put on SPARC 20)
32 MB RAM
2 GB HARD DISK SPACE. (This can, support up to 60 days archive and 1000 msgs per day.
larger sites may require more disk space.)
For AMHS another 1 MB for apps

B.1.2 Other Required Gccs Servers

Executive Manager Server
Sybase Database Server
Applix license Server
DNS Server
NIS + Server
Note these servers should be on line before you begin to install the AMHS server, the Executive Manager and Sybase Database can be on one server.

B.1.3 Software Required

Segments required for a new load:
DO NOT INSTALL FROM THIS LIST --FOLLOW THE PROCEDURES.

THE AMHS WILL NOT WORK IF YOU DON'T!

Order	Name	Date	Version
1	GCCS COE		X
2	EM V2.1 Upgrade	08/15/95	2.1.6
3	EM Printer Admin	01/12/96	2.1.9
4	Applix 3.2	01/12/95	3.2
5	Cmd Ctr Apps	08/05/95	2.1.5
6	CCAPPS AMHS Patch	10/25/95	1.0
7	COTS Topic	12/02/95	3.1.5c
8*	AMHS Server	08/05/95	2.1.4
9	AMHS Client	08/05/95	2.1.4
10	CCAPPS MM Patch	12/21/95	1.3
11	EM Launch Patch	12/27/95	1.1
12*	AMHS Server Patch	12/10/95	3.1
13	AMHS Client Patch	12/09/95	3.1

SAT PC: MS-6.2
PC-NFS 5.1
SAT-GR 4.10B

B.1.4 Information Required For Installation

A. Install Solaris 2.3 on AMHS Server.

[ ] IP Address of AMHS Server _____
[ ] Hostname of AMHS Server _____
[ ] IP Address of SAT _____
[ ] Hostname of SAT _____
[ ] IP Address of EM Server _____
[ ] Hostname of EM Server _____
[ ] IP Address of Sybase _____
[ ] Hostname of Sybase Server _____
[ ] IP Address of Applix Server _____
[ ] Hostname of Applix Server _____
[ ] Domain name _____
[ ] IP Address of DNS Server _____
[ ] Hostname of DNS Server _____
[ ] IP Address of NIS + Server _____
[ ] Hostname of NIS + Server _____
Password for sysadmin, secman, root on EM Server
Password for Sybase
Password for root, sysadmin, and amhs_dba on AMHS Server
[ ] Disk space required to store messages.
[ ] Own Station Routing Indicator (OSRI)
[ ] Destination Station Routing Indicator (DSRI)
[ ] Site Plain Language Address (PLA)
[ ] Applix license number for machines to have AMHS or AMHS clients.

B.1.5 Installation Procedures To Perform Before Starting Amhs Segment Tape Install.

A. Create amhserver alias (Set up NIS+ on amhserver)

[ ] Log into EMSERVER as root (NIS+ must be running).
Store old NIS+ table data into files (Optional)
- [ ] **nisaddent -d hosts | sort -t: 0+ -1 > hosts**<return>
- [ ] **nisaddent -d passwd | sort -t: 0+ -1 > passwd** <return>
- [ ] **nisaddent -d shadow | sort -t: 0+ -1 > shadow**<return>
- [ ] **nisaddent -d group | sort -t: 0+ -1 > group**<return>

[ ] Add amhserver to NIS+ host table:
- [ ] **cd /h/EM/nis_files**<return>
- [ ] **vi hosts** <return>
  - [ ] **G**<return> (Go to last line of file)
  - [ ] **o**<return> (Add a new line)
  - [ ] Enter the IP address and host name and alias of amhs server, sat and amhs clients.

    <u>This is an example enter YOUR IP Address and hostname and alias:</u>
    ***128.149.96.100 ga100* amhserver**
    ***128.149.96.101 ga101* sat**
    128.149.96.102 ga102 amhsclient
  - [ ] <ESC> **dd** (Exit from insert mode and delete last blank line)
  - [ ] **:wq!**<return>
- [ ] **/usr/lib/nis/nispopulate -F hosts**<return>

  The computer should respond with the following:
  NIS+ Domainname : *Domainname*
  Directory Path : *current directory*

Is this information correct? (Yor N) **Y**<return>
Example:
NIS+ Domainname : acom.nis
Directory Path : (current directory)

Is this information correct? (Y or N) Is this information correct? (Y or N) y

This script will populate the following NIS+ tables for domain acom.nis. from the files in current directory: hosts

Do you want to continue? (Y or N) y

populating hosts table from file ./hosts...
hosts table done.

Populating the NIS+ credential table for domain acom.nis.
from hosts table. The passwd used will be nisplus.

dumping hosts table ...
loading credential table...

The credential table for acom.nis has been populated.

Done!

B. Install NIS + on Client. Do this after GCCS has been installed on AMHS server.

[ ] Log in as root on amhserver
  [ ] **nisstat**<return> Check to see if machine has already been setup if not complete the following.
  [ ] Remove any old NIS+ information if it exists.
    [ ] **rm /etc/.rootkey**<return>
    [ ] **rm -rf /var/nis/***<return>
  [ ] **domainname**
    Make sure the name output is the same as the domainname.
    If not then
    echo `domainanme` > /etc/defaultdomain
  [ ] Initialize the client (amhserver)
  [ ] **nisclient -i - d *domainname* -h emserver**<return>

    The following appears on the screen:

    Please enter the network password that your administrator gave you.. **xxxxxxx** <return>
    Note: get xxxxxxx from GCCS install procedures or your site system administrator.

    Enter root login password: ***rootpassword***<return>

  [ ] **cp /h/EM/systools/nsswitch.EM /etc/nsswitch.conf**<return>

  [ ] Check the client's **/etc/nsswitch.conf** file:
    [ ] Ensure the entries for **passwd, group and hosts** look like the following:
      passwd: nisplus files
      group: nisplus files
      hosts: files dns nisplus [NOTFOUND = return]

C. Add AMHS DAC UNIX Groups

[ ] Log into EMSERVER as secman
[ ] double click on the icon security
  [ ] seclect **File -> Groups -> New**
  [ ] create the following groups:

NOTE: Add one group at a time and select "apply" until you get to the last group name, and then select "ok" after putting in the last group name.

NOTE: You will need to know the "sybase" SA name and password when adding groups.

Group Name	Group Number
topic	**200**
amh_cwp	**201**
amh_fbis	**202**
amh_excl	**203**
amh_limd	**204**
amh_nato	**205**
amh_pers	**206**
amh_spec	**207**
amh_ts	**208**
amh_rel	**209**

D. Add Initial AMHS Topic Administrator account

[ ] Log into the EMSERVER as secman
[ ] Create new user called amhs_dba
  [ ] click on **Security Icon and enter secman password when prompted in run_securitywindow**
  [ ] In **SECURITY MANAGER** window select **File -> Create Account**
    [ ] Userid (8 chars or less) i.e amhs_dba (must be amhs_dba)
    [ ] Username: **AMHS Administrator**
    [ ] user id #: (over ride previous number with **202**)
    [ ] At password prompt: **vinson** (or get password from sys admin)
    [ ] At the SyBase prompt for SA: **Enter name for Sybase SA**
    [ ] At the SyBase password prompt: **Enter password for SyBase SA**
    [ ] Default Group **gccs**
    [ ] Additional Group: **(Leave Blank)**
    [ ] Acct Group: **(GCCS Operator)**
    [ ] Role: (**GCCS Default)**
    [ ] Then select **"OK"**

E. Set up user groups.

[ ] Grant user access to the previously created AMHS DAC Groups
[ ] Select **File -> Groups -> Edit User's Groups**
  [ ] User: **amhs_dba**
  [ ] then click on groups to grant access
    add these groups: **topic, amh_cwp, amh_fbis, amh_excl, amh_limd, amh_nato, amh_pers, amh_spec, amh_ts, amh_rel, gccs, admin.**
  [ ] then click on **"ok"**

F. Set up correct home path for amhs server.

[ ] Modify NIS+ passwd table to give it the correct home path.
[ ] log onto Emserver as root
[ ] **nistbladm -m home=/h/AMHS/Server/topic/amhs_db/home **
'[name=amhs_dba,], passwd.org_dir'<return>
^--- single quote
[ ] verify the change using **niscat passwd.org_dir | grep amhserver**<return>

Create amhserver alias (Set up NIS+ on amhserver)
[ ] Log into EMSERVER as root (NIS+ must be running).
Store old NIS+ table data into files (Optional)
[ ] **cd /tmp**
[ ] **nisaddent -d hosts > hosts**<return>
[ ] **nisaddent -d passwd > passwd** <return>
[ ] **nisaddent -d shadow > shadow**<return>
[ ] **nisaddent -d group > group**<return>
[ ] vi the passwd file and change the home directory entry for amhs_dba to
/h/AMHS/Server/topic/amhs_db/home
[ ] **cp hosts /h/EM/nis_files/hosts**
[ ] **cp passwd /h/EM/nis_files/passwd**
[ ] **cp shadow /h/EM/nis_files/shadow**
[ ] **cp group /h/EM/nis_files/group**
[ ] **/usr/lib/nis/nispopulate -F -p /h/EM/nis_files -d `domainname`.**<return>
^ -- backticks & don't forget period

The computer should respond with the following:
NIS+ Domainname : *Domainname*
Directory Path : *current directory*

Is this information correct? (Yor N) **Y**<return>
Example:
NIS+ Domainname : acom.nis
Directory Path : (current directory)

Is this information correct? (Y or N) Is this information correct? (Y or N) y

This script will populate the following NIS+ tables for domain acom.nis. from the files in current directory: hosts

Do you want to continue? (Y or N) y

populating hosts table from file ./hosts...
hosts table done.

Populating the NIS+ credential table for domain acom.nis.
from hosts table. The passwd used will be nisplus.

dumping hosts table ...
loading credential table...

The credential table for acom.nis has been populated.

Done!

G. PCNFSD Setup on EMServer if EMServer has floppy drive. Use one of the three options below to copy files from the PC-NFS disk to EM Server.

[ ] Log in as root on Executive Manager
[ ] Insert diskette 5 of 5 of the Sun PC-NFS 5.1 disk set
[ ] **volcheck**<return> (mounts floppy)
[ ] **cd /floppy/sunpc-nfs/sunos.5x/sparc**<return>
[ ] **cp pkg.taz /var/spool/pkg**<return>
[ ] **cp addpkg.sh /var/spool/pkg**<return>

If EM Server does not have floppy drive use other machine on network.

[ ] Log in as root on machine with floppy drive
[ ] Insert diskette 5 of 5 of the Sun PC-NFS 5.1 disk set
[ ] **volcheck** (mounts floppy)
[ ] **cd /floppy/sunpc-nfs/sunos.5x/sparc**<return>
[ ] **cp pkg.taz /tmp**<return>
[ ] **cp addpkg.sh /tmp**<return>
[ ] Log in as root on Executive Manager
[ ] **rcp -p *hostname _of _computer_with_floppy*:/tmp/pkg.taz **
_hostname _of _emserver_:/var/spool/pkg <return>
[ ] **rcp -p *hostname _of _computer_with_floppy*:/tmp/addpkg.sh **
_hostname _of _emserver_:/var/spool/pkg <return>

If FTPing files from SAT.
[ ] Install PC-NFS on SAT -- See SAT Install procedures
[ ] Steps to log in to EM Server and FTP files from PC-NFS manual here tdd
Insure that the IP address, hostname and alias of EM server is in hosts file
[ ] Bring SAT PC up on network, ignore errors for mounting J drive , passwords etc.
[ ] Load disk five of the PC-NFS in floppy drive of SAT
[ ] **CD C:\NFS**<return>
[ ] **COPY a:\ sunpc-nfs\sunos.5x\sparc\ *.*** <return>
[ ] **ftp *emserver_hostname***<return>
the following or similar will appear
Connected to *hostname*
220 brady FTP server (UNIX( ) System Release 4.0) ready
Name (*hostname*:nobody): **amhs_dba**<return>
Password (*hostanme*:amhs_dba): ***amhs_dba_password***<return>
331 Password required for amhs_dba
230 User amhs_dba logged in
ftp> **bin**<return>
200 Type set to I
ftp> **put pkg.taz /var/spool/pkg/pkg.taz**<return>
200 Port Command Successful
150 Binary connection for /var/spool/pkg/pkg.taz
226 transfer complete
xxx bytes sent in yyy seconds
ftp> **put addpkg.sh /var/spool/pkg/addpkg.sh**<return>
200 Port Command Successful
150 Binary connection for /var/spool/pkg/pkg.taz
226 transfer complete
xxx bytes sent in yyy seconds
ftp> **bye**<return>

Install PC-NFSD on EM Server

[ ] Log in as root on Executive Manager
[ ] **cd /var/spool/pkg**<return>
[ ] **chmod +x addpkg.sh**<return>
[ ] **./addpkg.sh**<return>
[ ] **pkgadd**<return>

Answer the following questions to pkgadd.

The following packages are available:

1. SUNpcnfs PC-NFS Daemons: Enter **1**

Select package(s) you wish to process

[ ] Do you want to install the PC-NFS Daemon? Y
[ ] Do you want to install the Console Messaging server? N
[ ] Do you want to install the PC-NFS licensing? N
[ ] Do you want to install the PC-NFS Slip Driver? N

Note: If error message ... dup_grp_ent on any of the above options remove nisplus entries for passwd and grou in **/etc/nsswitch.conf** file. Re run the PCNFSD steps above and then restore nsswitch.conf file.

Turn on YP compatibility mode on the EM Server

[ ] **cd /etc/rc2.d**<return>
[ ] **vi S71rpc**<return>
[ ] Uncomment line that reads EMULYP = "Y"
[ ] **wq!** <return>
[ ] **init 6**

B.2 INSTALLATION OF SOFTWARE ON AMHS SERVER

B.2.1 Load Software.

[ ] Login as sysadmin on the amhserver.
[ ] Insert Segment tape in tape drive.
[ ] Launch SA Installer by clicking on the Install icon.
[ ] Click Select Media button
[ ] Select host that has the tape drive connected.
[ ] Select other in the Device window.
[ ] Click on the data entry line below other and enter **/dev/rmt/0mbn**
[ ] Click **"OK"**
[ ] Click **READ TOC** (read the table of contents)
** If error repeat steps starting with Click Select Media and enter **/dev/rmt/1mbn**
[ ] Install the following segments one at a time in the order listed as described in the detailed instructions listed in chapters three and four of the Implementation Procedures for GCCS Version 2.1.
NOTE: Do not load AMHS_UPDATE, this is for upgrading 2.0 AMHS systems to 2.1.4 only

[ ] Operating System	(Not a segment)
[ ] GCCS COE 2.1.0.2	
[ ] GCCS 2.1.0.2 Patch	1.0.0
[ ] GCCS 2.1.0.2 Patch 2	1.0.0.01
[ ] GCCS 2.2.0.2 Patch 4	1.0.1.02
[ ] APPLIX	3.2
[ ] EM 2	2.1.1

[ ] EM V2.1 Upgrade	2.1.6	8/15/95
[ ] EM Printer Admin	2.1.9	1/12/96**
** if you don't have version 2.1.9 then use 2.1.5		
[ ] Cmd Ctr Apps	2.1.5	8/5/95
[ ] CCAPPS AMHS Patch	1.0	10/25/95
[ ] COTS Topic	3.1.5.c	12/02/95
[ ] AMHS Server	2.1.4	08/05/95
[ ] AMHS Client	2.1.4	08/05/95
[ ] CCAPPS MM Patch	1.3	01/30/96
[ ] EM Launch Patch	1.1	12/27/95***
*** if you don't have this skip it and press on		
[ ] AMHS Server Patch	3.1	01/10/96
[ ] AMHS Client Patch	3.1	01/09/96

[ ] Auditing 2.1.1

IF UPGRADING AMHS 2.X TO 3.1 FOLLOW PROCEDURES TO CONVERT EXISTING 2.X ACCOUNTS TO 3.1 ACCOUNTS BEFORE STARTING AMHS SYSTEM ADMIN TOOL.

B.2.2 Set up AMHS directory.

Do either 1, 2, or 3 depending on system configuration.

1. Preparing new amhs disk out if the box.
   [ ] use implementation procedures to prepare new disk called /amhs.
   (**"format and newfs commands"** to partition disks.)

2. Modify exisitng disk configuration to acomodate amhs partition. The system might be already partitioned, but was not given the correct name **/amhs**, but was called somthing else i.e. /**home2**. This assumes /home2 is empty.
   [ ] log in as root
   [ ] **mkdir /amhs**
   [ ] **vi /etc/vfstab**
   [ ] change **home2** to **amhs**
   [ ] save file by typing **wq!**
   [ ] **mount /amhs**

3. Modify exisitng disk configuration to acomodate amhs partition. The system might be already partitioned, but was not given the correct name **/amhs**, but was called somthing else i.e. /**home2**. This assumes /home2 has segments loaded.

   [ ] The system was partitioned but had the following names:
   /h /home1 /home2. /home2 has 2 gig of space but it also has a subdirectory called UB under it.
   You will need to do the following:

.

   NOTE: do not use the "**rm**" command on segments.

   [ ] To move /UB do the following.

   [ ] log in as root
   [ ] **mkdir /home1/UB**
   [ ] **cd ./home2/UB**
   [ ] **find . -print | cpio -pdmuv /home/UB**
   [ ] **cd /**
   [ ] **rm -r /home2/UB**
   [ ] **rm /h/UB**

[ ] **ln -s /home1/UB /h/UB**
[ ] **mkdir /amhs**
[ ] **vi /etc/vfstab**
[ ] change **home2** to **amhs**
[ ] save file by typing **wq!**
[ ] **init 6**

B.2.3 Configure amhs directories and set up files on directories

1. Log in as root on the amhserver.

2. Create the following directories by performing the following steps:

   [ ] **mkdir /amhs/sat**<return>
   [ ] **mkdir /amhs/topic**<return>
   [ ] **mkdir /amhs/dac**<return>

3. Change ownership on the following directories by performing the following steps:

   [ ] **chown -R amhs_dba /amhs/sat**<return>
   [ ] **chown -R amhs_dba /amhs/topic**<return>
   [ ] **chown -R amhs_dba /amhs/dac**<return>

4. Change group ownership on the following directories by performing the following steps:

   [ ] **chgrp -R gccs /amhs/sat**<return>
   [ ] **chgrp -R gccs /amhs/topic**<return>
   [ ] **chgrp -R gccs /amhs/dac**<return>

5. Change permissions on the following directories by performing the following steps:

   [ ] **chmod -R 775 /amhs/sat**<return>
   [ ] **chmod -R 775 /amhs/topic**<return>
   [ ] **chmod -R 775 /amhs/dac**<return>

6. Check the above directories and ensure group, ownership, and permissions have indeed been changed.

   [ ] **ls -al /amhs | more**<return>
   [ ] Fix any problems with ownership, permissions, or with the group.

7. Copying sat, topic, and dac.

   [ ] **su - amhs_dba**<return>
   [ ] **cd /h/AMHS_SRV/sat**<return>
   [ ] **find . -print | cpio -pdmuv /amhs/sat**<return>
   [ ] **cd /h/AMHS_SRV/topic**<return>
   [ ] **find . -print | cpio -pdmuv /amhs/topic**<return>
   [ ] **cd /h/AMHS_SRV/dac**<return>
   [ ] **find . -print | cpio -pdmuv /amhs/dac**<return>
   [ ] **exit**<return>

8. Delete info from AMHS_SRV

[ ] **cd ../** <return>
[ ] **pwd**<return> -- should be **/h/AMHS_SRV**
[ ] **rm -r /h/AMHS_SRV/sat**<return>
[ ] **rm -r /h/AMHS_SRV/topic**<return>
[ ] **rm -r /h/AMHS_SRV/dac**<return>

9. Soft link on directory

[ ] **ln -s /amhs/sat /h/AMHS_SRV/sat**
[ ] **ln -s /amhs/topic /h/AMHS_SRV/topic**
[ ] **ln -s /amhs/dac /h/AMHS_SRV/dac**

10. Create AUTODIN directory for SAT on AMHS Server.

[ ] **cd /amhs/sat**
[ ] **mv autodin autodin.tlc**
[ ] **mkdir autodin**
[ ] **chown -R amhs_dba autodin**
[ ] **chgrp -R gccs autodin**
[ ] **chmod -R 775 autodin**

11. EXPORTING OTHER FILE SYSTEMS

[ ] **cd /etc/dfs**
[ ] **vi dfstab**
[ ] add the following line: **share -F nfs /amhs**
[ ] save file by typing **:wq!**
[ ] type on the command line: **share -F nfs /amhs**

B.2.4 SETTING UP PLAs, RI s, and Classification Marking PLAs

The Master PLA list is installed with the CCAPPS segment this should be verified with the sites PLA.

1. Default PLA for MTF editor. These steps must be performed on all AMHS clients.
   [ ] Login as root
   [ ] **/usr/asterix/asterix**
      [ ] *** -> Macro Editor**
         [ ] **File -> Open**
         [ ] **Directory -> h COTS APPLIX axlocal elf mtf_editor**
         Note: execute the Find command below from the menu bar.
         [ ] **Find -> Find & Replace**
            [ ] Find: **usr/edss/mount_point/pla_tables**
               Replace: **usr/edss/pla_tables**
            [ ] **Replace All**
            Note: include the quotes in the next find and replace operationj.
            [ ] Find: **"/usr/edss/pla_tables"**
               Replace: **"/usr/edss/pla_tables/New_PLAs"**
            [ ] **Replace All**
            [ ] **Cancel**

[ ] **File -> Compile & Save**
[ ] **File -> Exit**
[ ] **File -> Exit**
[ ] **vi /h/CCAPPS/data/config/Mv.CCA**
[ ] change last line from **MTF_SITE=SITE PLA in /h/CCAPPS/data/config/Mv.CCA**
to read: **MTF_SITE=***site PLA*
NOTE: Obtain site PLA from site Comm people
[ ] **:wq!**

2. Add site specific routing indicators.
[ ] **cd /h/data/global/EMDATA/pla_tables**
[ ] **vi Ri.CCA**
[ ] change **RUSNMHS** to *site OSRI*
[ ] change **RUSNSUU** to *site DSRI*
NOTE: Obtain site Own Station Routing Indicator (OSRI)
and Destination Station Routing Indicator (DSRI) from site Comm people
[ ] **:wq!**

3. Remove capability to have TOP SECRET Labels.
[ ] **vi Class.CCA**
[ ] delete the two lines that have top secret
CLASS = T, T O P S E C R E T
CLASS = T, TOP SECRET
[ ] **:wq!**

[ ] **vi MAST_PLA.CCA**
[ ] Insert command and site unique PLAs in alphabetical order to RIs listed in file. At least one of the PLAs should be the same entry as in the MTF_SITE = in the Mv.CCA file.
NOTE: Use **/^J** command to find beginning of "Js" in file to save paging through file
[ ] **:wq!**
[ ] **/h/CCAPPS/progs/create_pla_files**

[ ] Archive copies of modified mtf_editor.am, Class.CCA, and MAST_PLA.CCA to the amhs_install directory for future use.
[ ] **mkdir /h/data/global/EMDATA/amhs_install**
[ ] **cd /h/COTS/APPLIX/axlocal/elf/**
[ ] **cp mtf_editor.am /h/data/global/EMDATA/amhs_install**
[ ] **cd /h/data/global/EMDATA/pla_tables**
[ ] **pwd** should read **/h/data/global/EMDATA/pla_tables**
[ ] **cp * ../amhs_install**
[ ] **cd /h/CCAPPS/data/config/**
[ ] **cp Mv.CCA /h/data/global/EMDATA/amhs_install**

Identify processes for Executive Manager Server to monitor.

[ ] Login to amhserver as root
[ ] **cat /h/AMHS_SRV/data/config/active_spt.AMHS >>**
/h/data/global/EMDATA/config/active_spt
[ ] **vi /h/data/global/EMDATA/config/active_spt**
[ ] **ESC:1,$s/egret/"*amhserver-name*"/**
[ ] **ESC:wq!**
[ ] reboot emserver

B.3 INSTALLATION OF CLIENTS

B.3.1 Load Software.

[ ] Login as sysadmin on the client.
[ ] Insert Segment tape in tape drive.
[ ] Launch SA Installer by clicking on the Install icon.
[ ] Click Select Media button
[ ] Select host that has the tape drive connected.
[ ] Select other in the Device window.
[ ] Click on the data entry line below other and enter **/dev/rmt/0mbn**
[ ] Click **"OK"**
[ ] Click **READ TOC** (read the table of contents)
** If error repeat steps starting with Click Select Media and enter **/dev/rmt/1mbn**
[ ] Install the following segments one at a time in the order listed as described in the detailed instructions listed in chapters three and four of the Implementation Procedures for GCCS Version 2.1.

[ ] Operating System (Not a segment)			
[ ] GCCS COE 2.1.0.2			
[ ] GCCS 2.1.0.2 Patch		1.0.0	
[ ] GCCS 2.1.0.2 Patch 2		1.0.0.01	
[ ] GCCS 2.2.0.2 Patch 4		1.0.1.02	
[ ] APPLIX		3.2	
[ ] EM 2		2.1.1	
[ ] EM V2.1 Upgrade		2.1.6	8/15/95
[ ] EM Printer Admin		2.1.9	1/12/96**
[ ] Cmd Ctr Apps		2.1.5	8/5/95
[ ] CCAPPS AMHS Patch		1.0	10/25/95
[ ] COTS Topic		3.1.5.c	12/02/95
[ ] AMHS Client		2.1.4	08/05/95
[ ] CCAPPS MM Patch	1.3	01/30/96	
[ ] EM Launch Patch		1.1	12/27/95***
[ ] AMHS Client Patch		3.1	01/09/96
[ ] Auditing	2.1		

NOTE: After installing auditing 2.1.1 there will be message to run bsmconv in single user mode do ... **Wait till AMHS is operational before running bsmconv.** not start auditing untill after amhs is operational.

B.3.2 Install NIS + as client using implementation procedures.

[ ] **vi /etc/hosts**<return>
[ ] **nisclient -i -d *host-domainname* -h emserver**<return>

B.3.3 Add amhserver mount to /etc/vfstab file.

[ ] Login as root
[ ] **mkdir /amhs**<return>
[ ] **vi /etc/vfstab**<return>
[ ] Add the following line:
amhserver: /amhs - /amhs nfs -yes rw, bg, soft
[ ] **:wq!** <return>
[ ] **mount /amhs**<return>

B.3.4 Update local copies of mtf_editor.am and Mv.CCA files.

(The easiest way is to use copies from the amhs_install archive.)

[ ] Login into client as root
[ ] **cd /h/dat**a/global/EMDATA/amhs_install
[ ] **cp mtf_editor.am /h/COTS/APPLIX/axlocal/elf/**
[ ] **cp Mv.CCA /h/CCAPPS/data/config/**

B.4 INSTALLATION OF SOFTWARE ON SAT

B.4.1 Install PC-NFS Software on SAT

[ ] Insert PC-NFS Install diskette 1 into floppy drive.
[ ] **a:\install**
[ ] path to install PC-NFS : **C:\NFS**
[ ] answer yes to install utilities for DOS
[ ] answer yes to install telnet application for DOS
[ ] leave windows path blank (don't want to install windows software)
[ ] answer no to install windows utilities

The Installation summary screen should read as follows:

PC-NFS Installation Program

Summary of Answers to Install Questions

PC-NFS Path	: C:\NFS
DOS utilities?	: Yes
DOS Telnet Application?	: Yes
Windows utilities?	: No
Windows path	:

Disk Space Summary (Kbytes)

Basic PC-NFS	: 923
DOS utilities	: 1454
DOS Telnet application	: 759
Amount reserved for configuration	: xxx
Total amount required to install PC-NFS	: xxx
Total currently available on drive 'C"	: xxx
Total available after installation	: xxx

Note xxx n/a
Press enter to begin copying files. To change answer, use the PgUp Key

[ ] Press <enter>

[ ] Press any key to start the nfsconf program
[ ] Select NDIS driver
  [ ] Select other from driver menu
  [ ] Select NDIS
  [ ] Enter **C:\cpqnet** when prompted for path

Screen output will be:
Compaq Integrated Netflex ENET/PCI Controller
Drivername PCNTD$

[ ] Enter drive and path in which to copy the NDIS Driver
c:\lanman
[ ] Does your network contain DHCP? **N**
[ ] Choose correct time zone
[ ] Choose correct answer for daylight savings
[ ] Select name service in use on network **DNS**
[ ] Indicate letter of last drive for use by PC-NFS **Z**
[ ] Indicate whether RARP is in use on your network **N**
[ ] Indicate IP address of DNS server -- give IP address of emserver
[ ] Indicate DNS domain search path -- give DNS domainname
[ ] Indicate User name -- enter amhs_dba
[ ] Indicate name of PC -- give sat hostname
[ ] Indicate IP address of PC -- give IP address of SAT
[ ] Indicate pcnfsd server name -- **emserver**
[ ] Indicate IP address of pcnfsd server -- give IP address of emserver
[ ] Indicate name of gateway -- give gateway or router name
[ ] Indicate IP address of gateway -- give IP address of gateway
[ ] Indicate subnet mask

When asked to select method for obtaining license number select enter license number.
and at the prompt enter license number provided with PC-NFS.

Press enter to begin updating files.

NOTE: to change any of the above options at a later date
CD C:\NFS<return>
NFSCONF<return>
Press enter to reboot.

Setup Mount Point for SAT
[ ] **cd c:\nfs**<return>
[ ] add the following line to the drives.bat file:
NET USE J: amhserver:/amhs/sat /ms

B.4.2 Install SAT Software

[ ] reboot SAT
[ ] **J:** <return>
[ ] **CD AUTODIN**<return>
[ ] Insert SAT-GR Software disk in a: drive
[ ] **Copy a:*.*** <return>
[ ] Edit SAT.INI file
[ ] Change line that reads **MasterPath = E:\AUTODIN**<return>
to read **MasterPath = J:\AUTODIN**<return>
[ ] run plaedit to add site routing indicators
[ ] **plaedit**<return>
[ ] **Add**<return>
[ ] enter pla in data entry windows
[ ] **File -> Build**<return>
[ ] **Exit -> Save**<return>

[ ] run setup to configure SAT card. Parameter settings for MDT are listed below.
NOTE: EACH SETTING MUST MATCH THE SETUP OF THE MDT OR WHAT EVER AUTODIN SWITCH CONNECTED TO THE SAT
[ ] **J:** <return>
[ ] **CD AUTODIN**<return>
[ ] **J:\AUTODIN\SETUP**<return>
[ ] The following settings apply for an MDT connection with MDT supplying the clock signal

Base I/O Address:	300
Interrupt Vector:	5
Window Address	D800

****

1. OPERATING MODE [B]
   B = Block by Block
   C = Continuous

2. CRYPTO [N]
   N = None
   C = CAU/CCU/J-BOX
   K = KG 84

3. LINE MARKING [P]
   P = Positive (Mil-188)
   N = Negative (RS-232)

4. REP TIMER [L]
   L = LandLine
   S = Satellite

5. PREP SIGNAL STATE [+]
   + = (+6v) Asserted
   - = (-6v) Asserted

6. DATA INHIBIT SIGNAL STATE [+]
   + = (+6v) Asserted
   - = (-6v) Asserted

7. MODE - 1 CONNECTION [A]
   A = AUTODIN SWITCH
   F = AFAMPE
   L = LDMX
   M = AMME
   NOTE: Even if connected to AFAMPE use AUTODIN setting. AFAMPE setting forces SAT to output messages in DD-173 format.

****

1. OPERATING COMMUNITY [R]
   R = GENSER
   Y = DSSCS

2. HIGHEST PRECEDENCE [Z]
   W = CRITIC
   Y = EMERGENCY
   Z = FLASH
   O = IMMEDIATE
   P = PRIORITY
   R = ROUTINE

3. HIGHEST CLASSIFICATION [S]
   T = Top Secret
   S = Secret
   C = Confidential
   E = Unclassified EFTO
   U = Unclassified

4. T.I. LINE REQUIRED [N]
   Y = Yes
   N = No

5. CHANNEL ID Leave Blank
   Exactly 3 Alpha Char's

6. AUTO RETRY LIMIT [0]
   Maximum 3

7. ALARM ON IMMEDIATE PRECEDENCE [N]
   Y = Yes
   N = No

8. ARCHIVE SELF-TEST MESSAGES [N]
   Y = Yes
   N = No

9. MAGNETIC TAPE (9 TRACK) [N]
   Y = Yes
   N = No

10. PRINT TRANSMIT MESSAGES [D]
    D = Disable
    N = Narrative
    C = Card Format
    B = Narrative & CARD

11. DEFAULT OUTPUT FORMAT [J]
    D = DD173
    J = DOI - 103/JANAP128
    A = DOI - 103/ACP127

****

12. AUTO PRINT RECEIVE MSGS [N]
    Y = Yes
    N = No

13.	LOWER CASE SUPPORT Y = Yes N = No	[N]

****

1.	PC PRINTER OPTIONS P = Parallel 1 = COM1 Serial Port 2 = COM2 Serial Port	[P]

****

1.	OCR INSTALLED	[N]
2.	OCR TYPE	[D]
3.	OCR PORT	Leave Blank
4.	OCR Baud Rate	[4]

****

Set user account as prompted on last window of setup program.

B.4.3 The following sample files were copied from an operational system.

Settings for Ethernet Controller in Compaq PC.

Use F10 function key during boot to access setup program.

(PC should arrive configured this way, do not use pc configuration program unless you know what you are doing.)

Port Address	7000h - 7001Fh
Interrupt	3
Trigger	level

Settings for power management functions:

Disable all power management functions.

Settings for SCSI controller

Disabled.

SAMPLE CONFIG.SYS FILE

```
DEVICE=C:\DOS\HIMEM.SYS
dos=high
DEVICE=C:\DOS\EMM386.EXE NOEMS X=D000-E000
BUFFERS=20,0
FILES=35
DOS=UMB
LASTDRIVE=Z

REM *** The following block of lines was added by PC-NFS Configuration.***
DEVICE=C:\NFS\PCNFS.SYS /C^
DEVICEhigh=C:\NFS\SOCKDRV.SYS
```

DEVICEhigh=c:\lanman\PROTMAN.SYS /I:c:\lanman
DEVICEhigh=c:\lanman\NFS-NDIS.SYS
DEVICEhigh=c:\lanman\PCNTND.DOS
REM ***
FCBS=4,0
STACKS=9,256

SAMPLE AUTOEXEC.BAT FILE

SET PATH=C:\NFS;C:\CPQDOS;C:\;C:\DOS;
REM *** The following block of lines was added by PC-NFS Configuration.***
SET TZ=EST5EDT
SET NFSLANG=USA
SET NFSPATH=C:\NFS
C:\lanman\NETBIND
rem removed to conserve mem SET TN_DIR=C:\NFS\TELNET
rem removed to conserve mem C:\NFS\PRT *
C:\NFS\NET INIT
REM ***
SET PROMPT=PG
SET NWLANGUAGE=ENGLISH
J:
cd autodin
J:\autodin\sat_r

This note from PC-NFS readme.txt

5. PRINTING

MISLEADING INSTALLATION MESSAGE

If you do not include the PRT * statement in the AUTOEXEC.BAT file, you will get the error message:

> PC-NFS was not installed correctly
> No print redirector

You can ignore this message if you do not intend to use PC-NFS print services. You do not need the PRT * statement if you are not using PC-NFS print services.
We don't need the print services.

SAMPLE C:\NFS\DRIVES.BAT

NET USE J: ga5:/amhs/sat /ms,wsize=1024,rsize=1024

Sample C:\NFS\ETHERS

8:0:20:1:ab:cd sun-host
8:0:20:1:12:34 sun-server
2:60:8c:13:56:78 client-pc

Sample C:\NFS\HOSTS

```
156.316.45.30   gasat
156.316.45.10   ga10
156.316.45.30   gasat
156.316.45.5    ga5
156.316.45.28   gateway
```

Sample C:\NFS\NETWORK.BAT

```
NET NISDOMAIN hqaf.nis
NET START RDR gasat *
NET SUBNET 255.255.0.0
NET ROUTE gateway
NET NISSET ga10
NET PCNFSD ga10
NET LOGIN amhs_dba
```

Sample C:\LANMAN\PROTOCOL.INI

```
; This file was generated by PC-NFS NFSCONF
;
; Section for Protocol Manager
;
[PROTOCOL MANAGER]
 DriverName = PROTMAN$
;
; Section for  Compaq Integrated NetFlex ENET/PCI Controller
;
[PCNTND_NIF]
     DriverName = PCNTND$
;
; Section for PC-NFS NDIS Interface
;
[NFS-NDIS]
     DriverName = NFSLINK$
     Bindings = PCNTND_NIF
```

Sample SAT.INI File

```
[Site Specific Parameters]
; Where all SAT software is located ( i.e. C:\{GENSER} or C:\{DSSCS} )
MasterPath = J:\AUTODIN
; Up to 4 characters per entry, max 33 entries, separated by (,; )
; Leave blank if mail stops not required on print out.
MailStops = CCI RCI,AAAA;BBBB,CCCC,DDDD,EEE,FFF
; Number of days to maintain online archives
ArchiveAge = 30
; Validate PLA's during message preparation
PLAValidation = TRUE
; Expand narrative messages to 80 columns when copying to M/T
ExpandNarrativeMessage = FALSE
FormatLineValidation = 16
```

```
AlarmFrequency = 6000
MinPasswordLength = 8

[System Parameters]
ConfigurationFile = ccp.cfg
DownLoad = ccp2.bin
; For ASC installation only
;AutodinSwitch = TRUE
```

B.4.4 SAT - MDT Cable Interface

Note: use either port 2 or port 5 from MDT only.
Build either the adapter and use commercial cable, or build a custom cable and don't use the adapter.

Building an adapter:
1. The adapter consists of an RS232 DB9 (F) to DB25 (M) adapter and an RS-232 shielded jumper box. The jumper box is custom wired to support the SAT -- adapter -- MDT connection. The jumper box is not reversible, and requires the adapter to make the SAT-MDT connection work. The SAT and MDT sides SHOULD BE LABELED. The connections for the SAT, MDT, adapter, and jumper box are below.

MDT (DB9)		DB9/DB25		Adapter Jumper Box		SAT (DB25)	
Signal	pin	pin		MDT	SAT	Signal	pin
Transmit Clock	1	1	8	8	17	Rx Clk	17
Receive Data	2	2	3	3	2	Tx Data	2
Transmit Data	3	3	2	2	3	Rx Data	3
Gnd	4	n/c		nc	nc	n/c	
Gnd	5	5	7	7	7	Signal Gnd	7
Gnd	6	n/c		n/c	n/c	n/c	
Crypto Resync	7	n/c		n/c	n/c	n/c	
Inhibit Data	8	n/c		n/c	n/c	n/c	
Receive Clock	9	9	22	22	15	Tx Clk	15

Pin outs for custom cable:

MDT (DB9)		SAT (DB25)	
Signal	pin	Signal	pin
Transmit Clock	1	Rx Clk	17
Receive Data	2	Tx Data	2
Transmit Data	3	Rx Data	3
Gnd	4	n/c	
Gnd	5	Signal Gnd	7
Gnd	6	n/c	
Crypto Resync	7	n/c	
Inhibit Data	8	n/c	
Receive Clock	9	Tx Clk	15

B.4.5 SAMPLE MDT DECOM SETUP

Settings may be different if remoting link through crypto etc.

PORT: DCOM2 LABEL: GCCS BACKUP HOME enable: N
Maximum classification allowed on circuit: S Sanitization required: N
List of permitted SPACATs/SHDs: Rel Authority Required:N
Permitted TRC's: A: N, B: N, C: N, X: N, Z: N
Suppress SI/SO: N >Format: A (A=JANAP128, B=Format Line 1,
C=ACP127 US, D=ACP127 non-US)

Protocol: B (A= Not in use, B=Mode I)

Baud Rate: H (A= 75, B= 110, C= 150, D= 300, E= 600,
F=1200, G= 1800, H=2400, I= 4800)
Internal clock? Y (N=external clock) >Transmission Block by Block Y (N=continuous)

Repcount:0200

Also the MDT Software and jumpers should be set up as follows:
(See page 300-301 MDT manual)
Receive Data Polarity: Positive
Transmit Data Polarity: Positive
Transmit Clock Select: Internal
Receive Clock Select: Internal
Communications Mode select: Synchronous
External Clock Polarity: Positive (May not have this on your board)

B.5 START UP

[ ] Syncronize SAT, emserver, amhserver, and all amhs clients.
use date command on sun workstations
use both time and date command on SAT

[ ] reboot emserver, amhserver, and amhsclients
[ ] after amhserver and emserver are online, reboot sat by turning power off and then back on

NOTE: The topic processes have to be restarted any time the machine is rebooted
[ ] log on to the amhserver as amhs_dba
[ ] **cd ..**
[ ] **topic_cmd**
[ ] enter 1 to start topic processes
[ ] enter **.** to exit topic_cmd

CHECK OUT SYSTEM AS DESCRIBE IN AMHS SYSTEM ADMIN CLASS

AFTER SYSTEM IS WORKING ACTIVATE AUDITING PER GCCS IMPLEMENTATION PROCEDURES

B.6 DUAL SERVERS / ONE AS BACKUP

The following proceedure describes how to install the AMHS in a two server configuration with one server acting as a primary and the other acting as a secondary.

For purposes of these procedures, the primary server will have a hostname of ‘nmccamh1’ and the secondary server will have a hostname of ‘nmccdb2’. Of course, you should substitute the hostnames for your particular site.

The first step is to install and test each server independently as an AMHS server. Install the first server as instructed during the AMHS installation course. After the first server has been successfully installed and tested, start on the second server’s installation. Independently verify the second server’s installation by running the same tests performed on the first server. Remember to update the c:\nfs\drives.bat file on the SAT PC to point to the second server (reboot the SAT PC after making the change). Note: It is not necessary to update the ‘amhserver’ hostname alias to test the second server’s installation. The alias only needs to be change to test client workstations. Call if you have questions.

After testing both servers and verifying that both work independently as AMHS servers, the steps to configure them in a primary and secondary configuration can be performed. Do not perform the steps until both servers have been tested to work independently of each other. Note: Restore the c:\nfs\drives.bat file on the SAT PC before proceeding. Also, restore the ‘amhserver’ alias if changed to test client workstations.

The c:\nfs\drives.bat file on the SAT PC should always point to the primary AMHS server (in this case ‘nmccamh1’).

A. Specific Procedures for both servers:

Execute the following on both ‘nmccamh1’ and ‘nmccdb2’:

1) Login as the amhs_dba

2) Create the following directories:

```
mkdir   /amhs/sat/autodin/moved_tokens
mkdir   /amhs/sat/autodin/moved_tokens/bsq1
mkdir   /amhs/sat/atudoin/moved_tokens/bsq2
mkdir   /amhs/sat/autodin/moved_tokens/bsq3
mkdir   /amhs/sat/autodin/moved_tokens/bsq4
mkdir   /amhs/sat/autodin/moved_tokens/bsq5
```

3) Create the following soft link:

```
ln  -s   /amhs/sat/autodin/archive /amhs/sat/autodin/moved_tokens/archive
```

B. Specific Procedures for Primary Server (nmccamh1):

Execute the following procedures on the primary server (nmccamh1):

1) Login as the amhs_dba

2) Stop the AMHS server processes

3) Edit the vardef file:

vi /h/AMHS/Server/topic/amhs_db/vardef

4) This file contains a commented entry for a ‘move_token’ variable. Uncomment the entry and change the value:

move_token=/h/AMHS/Server/sat/autodin/moved_tokens/bsq3

C. Specific Procedures For Secondary Server (nmccdb2):

Execute the following procedures on the secondary server (nmccdb2):

1) Login as the amhs_dba

2) Stop the AMHS server processes

3) Edit the vardef file:

vi /h/AMHS/Server/topic/amhs_db/vardef

4) This file contains an entry for a ‘cfe_dir’ variable. Change to the following:

cfe_dir=/h/AMHS/Server/sat/autodin/moved_tokens

5) Edit the vfstab file:

vi /etc/vfstab

6) Add the following line to the vfstab file:

nmccamh1:/amhs/sat/autodin - /amhs/sat/autodin nfs - yes rw,bg,soft

7) Reboot the workstation.

B.6.1 Testing the Installation:

Testing the dual server configuration is very simple. Remember that the SAT terminal is the source of all incoming AMHS messages. Once a message is received at the SAT terminal, the primary server (nmccamh1) will process the message into its own Topic database. Once the message has been processed by the primary server (nmccamh1), the message will be passed to the secondary server (nmccdb2). The secondary server (nmccdb2) will process the message into its own Topic database. In other words, two separate Topic databases on two separate servers will be maintained as each message if received.

To test, start all the AMHS processes on both servers. Test the configuration by sending a test message into the system. This can be done by releasing a message from any client workstation or by sending a message from the SAT PC in loop back. Verify the message was received and processed by both AMHS servers by checking the AMHS message browsers from both the primary and the secondary servers. An AMHS message browser launched and displayed on the primary server will display messages from the primary Topic database. Likewise, an AMHS message browser launched and displayed on the secondary server will display messages that are on the secondary server's Topic database. The message should appear in both databases. Note: Come-back (CBC) copied will not appear in the secondary server's Topic database.

Running SW on remote machine and displaying desktop on local machine

1. Log in as root
2. xhost +
3. rlogin -l user_id remote_hostname (or ip_address)
4. edit .xsession comment line that reads setenv DISPLAY "`hostname`:echo $DISPLAY | cut -d: -f2 | cut -d. -f1`.0"
5. setenv DISPLAY local_hostname:0.0 (can use ip_address instead of local_hostname)
6. .xsession

NOTE: Must Start Off In xwindows Not Desktop.

B.7 PROCEDURES TO SET UP QUEUES FOR THE GRIS PROGRAMS

[ ] Login as root on the amhs server
[ ] chown amhs_dba amhs
[ ] chgrp gccs amhs
[ ] su - amhs_dba (and enter amhs_dba password)
[ ] cd /amhs
[ ] mkdir queues
[ ] cd queues
[ ] mkdir j36
[ ] cd /h/AMHS/Server/progs
[ ] create_queue j36 DIR /amhs/queues/j36 FILES
[ ] cd /h/COTS/Topic/current/bin
[ ] vi gris.otl

add the following lines

[ ] GRIS <sentence>
[ ] * "RECON"
[ ] * "REPORTID"

exit vi

[ ] cp gris.otl /h/AMHS/Server/topic/amhs_db/pf0topic/gris.otl
[ ] cd /h/AMHS/Server/progs
[ ] profile_queue j36 /h/AMHS/Server/topic/amhs_db/pf0topic/gris.otl
The following should be output to the screen
/h/COTS/Topic/current/bin/mkusrtop -q -u /h/AMHS/Server/topic/amhs_db/pf0topic -s
/h/AMHS/Servertopic/amhs_db/systopic -o /h/AMHS/Server/topic/amhs_db/pf0topic/QUEUE-1

mkusrtop -Version 3.1.5 (-ss0l22, Rev C Mar 8 1994)
mkusrtop done
/h/COTS/Topic/current/bin/rtsend /h/AMHS/Server/topic/amhs_db/mailbox pf0 NEWPROF
rtsend Version 3.1.5 (-ss0122, Rev C Mar 8 1994)
rtsend done

Check Out:
[ ] Login as a user with amhs release authority
[ ] Create a message with the words RECON and REPORTID in the same line
[ ] Release the message
[ ] Verify amhs placed a copy of the message in /amhs/queues/j36

(This procedure has been verified at CENTCOM and the OSF Integration Lab)

B.8 CONVERTING EXISTING 2.X AMHS ACCOUNTS TO 3.X ACCOUNTS

The first part of this is checklist install instructions, greater detail is provided in the system admin manual.

If there is a difference between the command in these procedures and the manual then these procedures should be followed.

login as root
cd /etc
vi passwd
delete amhs_dba line
save file

vi shadow
delete amhs_dba line

chown amhs_dba control.rts
chgrp gccs control.rts

vi group
delete topic line and all amhs groups

exit (to amhs_dba)

B.8.1 CONFIGURE SA TOOL TO MONITOR AMHS SERVER PROCESSES

[ ] cd /h/AMHS/Server/data
[ ] cd config
[ ]vi MainWindow.ini
[ ] change

PROCESSOR_ENTRY=AMHS Server, sun3

to

PROCESSOR_ENTRY=AMHS Server(*hostanme*), *hostname*

Configure .rhosts files to authorize SA Tool ICON on Desktop

[ ] cd /h/AMHS/Server/topic/amhs_db/home
[ ] vi .rhosts
[ ] add host name and account name for each account and host where the tool will be authorized

example
alpine steve
amhssvr steve
alpine jane (see section 5.1.1 in admin manual)

[ ] Load Client Patch on EM Server.

Work around if can't access server
login to emserver as sysadmin
cd /tmp
mkdir data
mkdir data/Profiles
cd data/Profiles
ftp amhshostname as amhs_dba
cd /h/AMHS_CLT_PATCH
cd data/Profiles
get LaunchDesc.AMHSC
get Profiles.AMHSC
bye
cd /tmp
setenv SESSION 0
/h/EM/progs/load_profiles data/Profiles/Profiles.AMHSC

Add AMHS System Admin Tool To System Administrators GCCS Desktop
[ ] Login AMHS Server as secman
[ ] run profile manager
[ ] modify->user->launch
[ ] add AMHS Administration
[ ] ok
[ ] exit profiler
[ ] exit secman
[ ] verify that **/h/AMHS/Server/topic/amhs_db/daclist** has the entries exactly as the below list.
If not then modify the file
/h/AMHS/Server/data/admin/SecurityValues to match the daclist see detailed tool configuration notes at the end of these procedures.

```
0=general
1=CWP
2=fbis
3=exclusive for
4=limdis
5=nato
6=nocon
7=personal for
8=specat
9=top secret
10=
11=
12=
13=
14=
15=
```

Make a backup copy of the current Topic password file.

[ ] cd /h/AMHS/Server/topic/amhs_db/password

[ ] cp password password.backup

Create a new UserAccountList file.

[ ] cd /h/AMHS_SERVER_PATCH/Scripts

[ ] ./ CreateAccountList

[ ] cd /tmp

[ ] vi UserAccountList

[ ] Check account listed make sure they are correct

[ ] add amhs_dba account - add line that reads

amhs_dba:1:::habyes:YES:0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15:

Copy the new UserAccountList file to the /h/AMHS/Server/data/admin directory.

[ ] **cp /tmp/UserAccountList /h/AMHS/Server/data/admin/**

Create a new Topic password file. Start with a blank Topic password file.

[ ] **cd /h/AMHS_SERVER_PATCH/templates**

[ ] **cp Topic_Password /h/AMHS/Server/topic/amhs_db/password/password**

Add password entries for each Topic user account.

[ ] **cd /h/AMHS/Server/Scripts/admin/**

[ ] Execute the following AddUser command for each Topic user account that appears in the newly created UserAccountList file. Replace the <username> argument with the actual name of your user.

su root (enter root password)

./AddUser <username> example: ./AddUser GCCSGCCSUSER

./AddUser <username> example: ./AddUser amhs_dba

NOTE: MUST ADD ALL THE USERS OR DON'T ADD ANY AND USE THE SA TOOL TO ADD THE USERS.

Compile the new Topic password file.

[ ] **su - amhs_dba** (enter amhs_dba password)

[ ] **cd /h/AMHS/Server/topic/amhs_db/password/**

[ ] **mkpwd password**

[ ] **cp /h/COTS/Topic/current/bin/topic31.pwd **
/h/AMHS/Server/topic/amhs_db/password/topic31.pwd

Patch the amhs_dba topic preference file.

[ ] **cd /h/AMHS_SERVER_PATCH/data/amhs_dba**

[ ] **cp topic.prf /h/AMHS/Server/topic/amhs_users/amhs_dba/**

Execute the following steps to create a new QueueInformation file.

Prepare a backup copy of your current profiles file.

[ ] **cd /h/AMHS/Server/topic/amhs_db/pf1topic**

[ ] **cp profiles profiles.backup**

Create a new QueueInformation file.

[ ] **cd /h/AMHS_SERVER_PATCH/Scripts**

[ ] **./CreateQueueInformation**

[ ] **more /tmp/QueueInformation** make sure entries are correct

Executing this script will create a QueueInformation file in the /tmp directory. This file should be inspected to make certain it agrees with the previously mentioned description of the QueueInformation file. There should be one entry for each Topic user account. The script only completes fields 1, 2, 3, 5, 7, and 9. Fields 4, 6, and 8 will have an x, y, and z respectively.

Completion of fields 4, 6, and 8 of the QueueInformation file are made using the Queue Manager Tool. Refer to the section of the system administration manual on using the Queue Manager Tool for an explanation on assigning Topic names to user queues. This step is performed after these setup procedures are complete.

Copy the QueueInformation file to the working directory.

[ ] **cp /tmp/QueueInformation /h/AMHS/Server/data/admin/**

Create a new profiles file. Start with the provided template.

[ ] **cd /h/AMHS_SERVER_PATCH/templates**

[ ] **cp Topic_Profiles /h/AMHS/Server/topic/amhs_db/pf1topic/profiles**

This completes the configuration of the Topic password and UserAccountList files. From this point forward, the Topic password and the UserAccountList file should not be edited unless instructed by a technical support representative. All future changes to these files is completely managed by the Account Manager Tool of the system administration tool.

[ ] Assign topic profiles to existing accounts using the queue manager function from the amhs system admin tool as described in section 5.5 of amhs sys admin manual.

[ ] Assign groups to the accounts using the account manager function from the amhs system admin tool as described in section 5.6 of the amhs system admin manual.

B.9 UPGRADING 3.0 AMHS TO 3.1 AMHS

Consists of saving config files restoring them after loading three patches.

[ ] **cd /tmp**
[ ] **su** and enter root password
[ ] **mkdir amh_home**
[ ] **mkdir amh_admin**
[ ] **mkdir amh_config**
[ ] **mkdir amh_dba**
[ ] **cd /tmp/amh_home**
[ ] **cp /h/AMHS/Server/topic/amhs_db/home/.cshrc .**
[ ] **cp /h/AMHS/Server/topic/amhs_db/home/.rhosts .**
[ ] **chown amhs_dba ***
[ ] **chgrp gccs ***
[ ] **cd ..**
[ ] **cd /tmp/amh_admin**
[ ] **cp /h/AMHS/Server/data/admin/* .**

files copied
DayNumber
DocumentSources
QueueInformation.previous
SecurityValues
SequenceNumber
UserAccountList

[ ] **chown amhs_dba ***
[ ] **chgrp gccs ***
[ ] **cd**
[ ] **cd /tmp/amh_config**
[ ] **cp /h/AMHS/Server/data/config/* .**

files copied
AccountManager.ini
AmhsAdmin.ini (*delete this or backup manager won't work)*
CustomLaunch.ini
DacManager.ini
MainWindow.ini
QueueManager.ini
ScriptLibrary.ini
active_spt.AMHS
mq.ini

[ ] **chown amhs_dba ***
[ ] **chgrp gccs ***
[ ] **rm AmhsAdmin.ini**
[ ] **cd /tmp/amh_dba**
[ ] **cp /h/AMHS/Server/topic/amhs_db/control.rts .**
[ ] **cp /h/AMHS/Server/topic/amhs_users/amhs_dba/topic.prf .**
[ ] **chown amhs_dba ***
[ ] **chgrp gccs ***

Load Software.

[ ] Login as sysadmin on the amhserver.
[ ] Insert Segment tape in tape drive.
[ ] Launch SA Installer by clicking on the Install icon.
[ ] Click Select Media button
[ ] Select host that has the tape drive connected.
[ ] Select other in the Device window.
[ ] Click on the data entry line below other and enter **/dev/rmt/0mbn**
[ ] Click **"OK"**
[ ] Click **READ TOC** (read the table of contents)
** If error repeat steps starting with Click Select Media and enter **/dev/rmt/1mbn**

[ ] CCAPPS MM Patch	1.3	01/30/96
[ ] AMHS Server Patch	3.1	01/10/96
[ ] AMHS Client Patch	3.1	01/09/96

Restore Config Files.

[ ] **cd /h/AMHS/Server/topic/amhs_db/home**
[ ] **cp /tmp/amh_home/.cshrc .**
[ ] **cp /tmp/amh_home/.rhosts .**
[ ] **cp /tmp/amh_dba/control.rts /h/AMHS/Server/topic/amhs_db/control.rts (Check directory tdd)**
[ ] **cp /tmp/amh_dba/topic.prf /h/AMHS/Server/topic/amhs_users/amhs_dba/topic.prf**
[ ] **cd /h/AMHS/Server/data/admin**
[ ] **cp /tmp/amh_admin/* .**
[ ] **cd /h/AMHS/Server/data/config**
[ ] **cp /tmp/amh_config/* .**

B.10 REMOTE FUNCTIONAL CHECKOUT TEST

B.10.1 Test Description

Test Accounts: The site will add the two user accounts jitc1 and jitc2. Passwords for the accounts will be arranged prior to the test via secure phone or via the GCCS Chat function.

jitc1: The account jitc1 will have the project position pair: Project - TEST, Position - USER1. The account will have the following launch icons: AMHS Client, MTF Editor, and Message Manager.
The user jitc1 will also have message release authority access to the LIMDIS, and Code Word Protect (CWP) Discretionary Access Code(DAC) accounts. Finally the jitc1 account will be profiled to receive all messages with the special handling codes of LIMDIS, NOFORN, and the Standard Subject Indicator Code (SSIC) of N02000, and the Plain Language Address (PLA) of GCCS USER ONE, or the RI of RHSSEBA.

jitc2: The account jitc2 will have the project position pair: Project TEST, Position - USER2. The account will have the following launch icons: AMHS Client, MTF Editor, and Message Manager.
The user jitc2 will not have message release authority or access to messages with the DAC of LIMDIS. The user jitc2 will have access to the Code Word Protect account. Finally jitc2 will be profiled to receive all messages with the Code Word SIDEKICK, SSIC code of N02030, PLA of GCCS USER TWO, or the RI of RHSSEBB.

Site Plain Language Addresses and Routing Indicators: The site shall have the two PLAs of GCCS USER ONE and GCCS USER TWO. The Routing Indicator (RI) of GCCS USER ONE will be RHSSEBA. The RI of GCCS USER TWO will be RHSSEBB. The GCCS USER ONE - RHSSEBA PLA-RI pair will be the default for the site.

Special Handling and Standard Subject Indicator Codes: The any of the following combinations may be used during the functional checkout test.

CONFIDENTIAL SIDEKICK
C O N F I D E N T I A L SIDEKICK
CONFIDENTIAL SIDEKICK //N02030//
C O N F I D E N T I A L SIDEKICK //N02030//
SECRET LIMDIS
S E C R E T LIMDIS
SECRET LIMDIS //N02000//
S E C R E T LIMDIS //N02000//

AMHS AUTODIN Connection: The AMHS SAT will be terminated with a loop back connector (not connected to AUTODIN) and in the ONLINE mode.

Functional Testing: Once the site has set up the AMHS for the test they should contact Maj. Dorsey (DNS 653 - 8588) and a date and time will be coordinated with the JITC tester to log in to the site's AMHS remotely from the OSF. The JITC tester will log in to the AMHS as jitc1, create and send messages, verify that the messages are correctly profiled, and perform other optional testing. The JITC tester will also log in as jitc2 and verify jitc2 has no release authority, no access to messages with the LIMDIS code words, that messages are profiled correctly for the account and other optional testing.

Post Test: Test accounts should be deleted immediately following test completion. If the test is successful and the site has submitted it's site description document a Component Approval Deployment Notice (CDAN) will be issued by the DMS office. While waiting for the CDAN the site may elect to connect to AUTODIN with the approval of the local Designated Approval Authority (DAA) for the site.

B.10.2 Procedures To Configure AMHS For Test

Create Project Position Pairs

[ ] Run Profile Manager
- [ ] **File -> New -> Project**
- [ ] Enter **TEST** for project name and click ok
- [ ] **File -> New -> Position**
  - [ ] Click on arrow button right of project name and select **TEST** from pull down list
  - [ ] Click OK and enter **USER1** in Position Name Field & Click OK.
- [ ] **File -> New -> Position**
  - [ ] Click on arrow button right of project name and select **TEST** from pull down list
  - [ ] Click OK and enter **USER2** in Position Name Field & Click OK.

NOTE: Ignore the error message in the run_profile window that reads:
sh: /usr/edss/admin/security_scripts/add_topic_user: not found

Define Launch Windows for Project-Project Pair

[ ] Still in Profile Manager
- [ ] **Modify -> Position -> Launch List**
- [ ] Click arrow button for Position Field
- [ ] Select **TEST.USER1**from pull down list
  - [ ] Assign **MTF Editor**, **Message Manager**, and **AMHS Client** to Position.
  - [ ] Click OK
- [ ] **Modify -> Position -> Launch List**
- [ ] Click arrow button for Position Field
- [ ] Select **TEST.USER2** from pull down list
  - [ ] Assign **MTF Editor**, **Message Manager**, and **AMHS Client** to Position.
  - [ ] Click OK

Create Test Accounts

[ ] Run SECURITY
- [ ] **File -> Create -> Account**
  - USER ID: j**itc1**
  - USER NAME: **JITC Remote AMHS Tester**
  - USER NUMBER: Accept number generated by SECMAN
  - PASSWORD:
  - SYBASE SYSTEM ADMNISTRATOR USER NAME:
  - SYBASE SYSTEM ADMNISTRATOR USER PASSWORD:
  - DEFAULT GROUP: **gccs**
  - OPTIONAL GROUPS: Leave Blank
  - ACCT_GROUP: **GCCS Operator**
  - ROLE: **GCCS Default**
  - & Click OK
- [ ] **File -> Create -> Account**
  - USER ID: j**itc2**
  - USER NAME: **JITC Remote AMHS Tester**
  - USER NUMBER: Accept number generated by SECMAN

PASSWORD:
SYBASE SYSTEM ADMNISTRATOR USER NAME:
SYBASE SYSTEM ADMNISTRATOR USER PASSWORD:
DEFAULT GROUP: **gccs**
OPTIONAL GROUPS: Leave Blank
ACCT_GROUP: **GCCS Operator**
ROLE: **GCCS Default**
& Click OK

Setup Groups for Accounts

[ ] Still in SECMAN
- [ ] **File -> Groups -> Edit User's Groups**
  - [ ] Click arrow button on user name, select **jitc1** and click ok
  - [ ] assign amh_limd, amh_rel, amh_cwp, and topic
  - [ ] Click OK

- [ ] **File -> Groups -> Edit User's Groups**
  - [ ] Click arrow button on user name, select **jitc2** and click ok
  - [ ] assign amh_cwp, and topic
  - [ ] Click OK

Link accounts with project - position pairs

[ ] From Profile Manager
- [ ] **File -> New -> User Profile**
- [ ] Click on arrow button next to User Id, select **jitc1**, and click ok
- [ ] Click on arrow button next to Project Name, select **TEST**, and click ok
- [ ] Click on arrow button next to Position Name, select **USER1**, and click ok
- [ ] Click ok

[ ] From Profile Manager
- [ ] **File -> New -> User Profile**
- [ ] Click on arrow button next to User Id, select **jitc2**, and click ok
- [ ] Click on arrow button next to Project Name, select **TEST**, and click ok
- [ ] Click on arrow button next to Position Name, select **USER2**, and click ok
- [ ] Click ok

Set up site default PLA

[ ] **vi /h/CCAPPS/data/config/Mv.CCA**
- [ ] change last line from **MTF_SITE=whatever???**
  to read: **MTF_SITE=GCCS USER ONE**
- [ ] **:wq!**

Set up site default RI

[ ] **vi /h/data/global/EMDATA/pla_tables/Ri.CCA**
- [ ] Change both RIs to RHSSEBA

Set up Special Handling and SSIC Codes

[ ] **vi /h/data/global/EMDATA/pla_tables/Class.CCA**
  [ ] Add the following lines.
    CLASS=C,CONFIDENTIAL SIDEKICK
    CLASS=C,C O N F I D E N T I A L SIDEKICK
    CLASS=C,CONFIDENTIAL SIDEKICK //N02030//
    CLASS=C,C O N F I D E N T I A L SIDEKICK //N02030//

    CLASS=S,SECRET LIMDIS
    CLASS=S,S E C R E T LIMDIS
    CLASS=S,SECRET LIMDIS //N02000//
    CLASS=S,S E C R E T LIMDIS //N02000//

Set up PLA tables

[ ] **vi /h/data/global/EMDATA/pla_tables/MAST_PLA.CCA**
  [ ] add **GCCS USER ONE** and **GCCS USER TWO** in alphabetical order
  [ ] **:wq!**
[ ] **/h/CCAPPS/progs/create_pla_files**

[ ] add the RIs to the SAT PLA tables, use PLAEDIT.EXE in J:AUTODIN from SAT Terminal.

Set up Topic Accounts

[ ] login the amhs server as amhs_dba
[ ] vi .cshrc and add second line to file that reads **umask 2**

[ ] **topic_cmd**
  [ ] **31** Shutdown topic processes
  [ ] **65** Add New Topic User
      enter **TEST** for the project
      enter **USER1** for the position
  [ ] **65** Add New Topic User
      enter **TEST** for the project
      enter **USER2** for the position
  [ ] **67** Update Password File

  [ ] **62** Edit password file. Note this calls the vi editor to edit password file

      Give jitc1 access to LIMDIS and CWP (SIDEKICK) topic accounts
      Arrow down to line that reads
      # Project/Position: TEST__USER1
      change line that reads /groups = 0 to read **/groups = 0, 1, 4**

      Give jitc2 access to CWP (SIDEKICK) topic account
      Arrow down to line that reads **#Project/Position: TEST__USER2**
      change line that reads /groups = 0 to read **/groups = 0,1**

      <esc>wq!

  [ ] **67** Update password file
  [ ] **1** Start Topic Processes
  [ ] **.** (Exit topic_cmd)

Add Code Word SIDEKICK to the Code Word Protect DAC group

[ ] **vi /h/AMHS/Server/topic/amhs_db/daclist**
- [ ] arrow down to line that reads "CWP"@
- [ ] change "CWP"@ to read **"SIDEKICK"@**
- [ ] **<esc>wq!**

[ ] **topic_cmd**
- [ ] **41** Stop satfeed
- [ ] **42** Stop cbcfeed
- [ ] restart both the satfeed and cbc feed
- [ ] exit topic_cmd

Setup topic profiles

[ ] **cd /h/AMHS_SRV/topic/amhs_users/amhs_dba**
[ ] **/usr/bin/X11/xset +fp /h/COTS/Topic/xfonts/pcf/default**
[ ] **/h/COTS/Topic/current/bin/xtopic** (start up topic client)
- [ ] **File -> New Query**
  - [ ] **Query -> Assists**
    - [ ] Select TEST__USER1-a
    - [ ] **File -> Open Topic Query**

Create Topic Profile as taught in system admin workshop profile jitc1 (TEST_USER1) to receive all messages with the special handling codes of LIMDIS, NOFORN, and the Standard Subject Indicator Code (SSIC) of N02000, the Plain Language Address (PLA) of GCCS USER ONE and the RI of RHSSEBA.
[See hint below]

<> TEST__USER1-a <any>---<> USER1-a <Sentence> <> ---<Word> TO
| |
| <Word> USER1
|
<> PLA <sentence> GCCS USER ONE <Phrase>
|
<> SECRET-LIMDIS <Sentence> <> SEC-Phrase <any> ---<Word> SECRET
| |
| <S E C R E T> <Phrase>
|
<> LIMDIS-SSIC <Sentence> <> ---<Word> LIMDIS
|
| <Word> N02000

Don't Forget NOFORN and the RI!

- [ ] **File -> Save Topic**

- [ ] **File -> New Query**
  - [ ] **Query -> Assists**
    - [ ] Select TEST__USER2-a
    - [ ] **File -> Open Topic Query**

Create Topic Profile as taught in system admin workshop profile jitc2 (TEST_USER2) to receive all messages with the special handling codes of SIDEKICK, and the Standard Subject Indicator Code (SSIC) of N02030, the Plain Language Address (PLA) of GCCS USER TWO and the RI of RHSSEBB.

[ ] **File -> Save Topic**

[ ] Exit Topic
[ ] **topic_cmd**
[ ] **33** Shutdown profiler
[ ] Shut down **pf1**
[ ] **3** Start profiler
[ ] Start **pf1**

B.10.3 TEST STEPS AT OSF

[ ] Set up the local machine to receive remote display

1. Log in as dorsey
[ ] **xhost +**

[ ] Set up remote amhs jitc1 account to display on local machine

[ ]. **rlogin -l jitc1** ***ip address for remote host*** **<RET>** (address for ACOM amhs is 157.224.130.5)
[ ] edit .xsession comment line that reads setenv DISPLAY "`hostname`:echo $DISPLAY | cut -d: -f2 | cut -d. -f1`.0"
[ ] **vi .xsession**
[ ] use down arrow key to move to line that reads
setenv DISPLAY "`hostname`:echo $DISPLAY | cut -d: -f2 | cut -d. -f1`.0"
[ ] type **i#<ESC>wq!**

[ ] **setenv DISPLAY** ***local_IP_address*****:0.0**

[ ] Start desktop for jitc1 account

[ ] **.xsession** (note: must start off in xwindows not desktop)
Go get cup of coffee

[ ] Check to insure desktop shows user id = jitc1, project=TEST, and position=USER1
(if project position pair shows GCCS GCCS USER try changing to TEST USER1)

[ ] Verify MTF Editor launches

[ ] Verify default PLA and RI are GCCS USER ONE and RHSSEBA

[ ] Create Free Text Message with secret classification and SSIC of 02000
To PLA: GCCS USER ONE
Subject: UNCLASSIFIED TEST MESSAGE MSG4
Declas: UPON RECEIPT
[ ] Save as Msg4

[ ] Create Free Text Message with confidential classification and SSIC of 02030
To PLA: GCCS USER TWO
Subject: UNCLASSIFIED TEST MESSAGE MSG5
Declas: UPON RECEIPT

[ ] Save as Msg5

[ ] Create Free Text Message unclassified
Subject: UNCLASSIFIED TEST MESSAGE MSG3
To PLA: GCCS USER TWO

[ ] Save as Msg3

[ ] Exit MTF

[ ] Launch Message Manager.

[ ] Create Buck Slip

[ ] Attach Msg5, Msg6, Msg3 to buck slip.

[ ] Open MSG4,
1. Edit classification line to S E C R E T LIMDIS //N02000//
2. Save
3. Edit subject line to UNCLASSIFIED TEST MESSAGE SEC LIM MSG1
4. Delete //N02000// from the classification line and save as MSG1

[ ] Open MSG5,
1. Edit classification line to C O N F I D E N T I A L SIDEKICK //N02030//
3. Save
2. Edit subject line to UNCLASSIFIED TEST MESSAGE CONF MSG2
4. Delete //N02030// from the classification line and save as MSG2

[ ] Open MSG3

1. Edit subject line to UNCLASSIFIED TEST MESSAGE UNC NOFORN MSG6
2. Save as MSG6

[ ] Attach MSG1, MSG2, MSG6 to Buckslip

[ ] Release MSG1, MSG2, MSG3, MSG4, MSG5, MSG6.
Note: amhs will automatically validate before releasing.

[ ] Open AMHS Client

[ ] Verify correct profiling of messages. Action queue should have messages 1,2,3,4,5, and 6

[ ] Exit

[ ] Set up remote amhs jitc2 account to display on local machine

[ ]. **rlogin -l jitc2** ***ip address for remote host*** **<RET>**
[ ] edit .xsession comment line that reads setenv DISPLAY "`hostname`:echo $DISPLAY | cut -d: -f2 | cut -d. -f1`.0"
[ ] **vi .xsession**
[ ] use down arrow key to move to line that reads
setenv DISPLAY "`hostname`:echo $DISPLAY | cut -d: -f2 | cut -d. -f1`.0"
[ ] type **i#<ESC>wq!**

[ ] **setenv DISPLAY *local_IP_address*:0.0**

[ ] Start desktop for jitc2 account

[ ] **.xsession** (note: must start off in xwindows not desktop)
Go get cup of coffee

[ ] Create Free Text Message unclassified
Subject: UNCLASSIFIED TEST MESSAGE JITC2 MSG7
To PLA: GCCS USER ONE

[ ] Save as Msg7

[ ] Open Message Manager

[ ] Create Buckslip

[ ] Attach MSG7

[ ] Open MSG7

[ ] Exit Applix

[ ] Verify jitc2 does not have release authority

[ ] Exit MM

[ ] Open AMHS Client, and verify correct profiling
Action queue should have Messages 2,3,5, and 6.

C. APPENDIX - GCCS SYSTEM ADMIN TOOLS

The GCCS AMHS is built on the GCCS COE and depends upon several system features for configuration and operation. The details of the operation are in the GCCS System User Manual #LL-500-133-01, System Administrator responsibilities, processes and methods are described in the GCCS Administration Manual #LL-500-29-06 and security issues are discussed in #LL-500-76-04, the Security Planning Manual. This appendix distills the GCCS EM Server contingent processes that are required for AMHS operation.

Each AMHS user, operator and administrator must have a unique GCCS account. This account is the same as their normal GCCS account but still must be added to a discretionary access control (DAC) group via Security Manager. Using Profile Manager, everyone must be issued a minimum of one project and one position (project/position pair). Proper group membership is essential to proper AMHS interaction.

System Monitor and Control can be configured to support AMHS functions, and the AMHS relies on the foldering system for message forwarding and user electronic filing. The GCCS desktop foldering system stores data in the Sybase SQL database.

C.1 SECURITY MANAGER

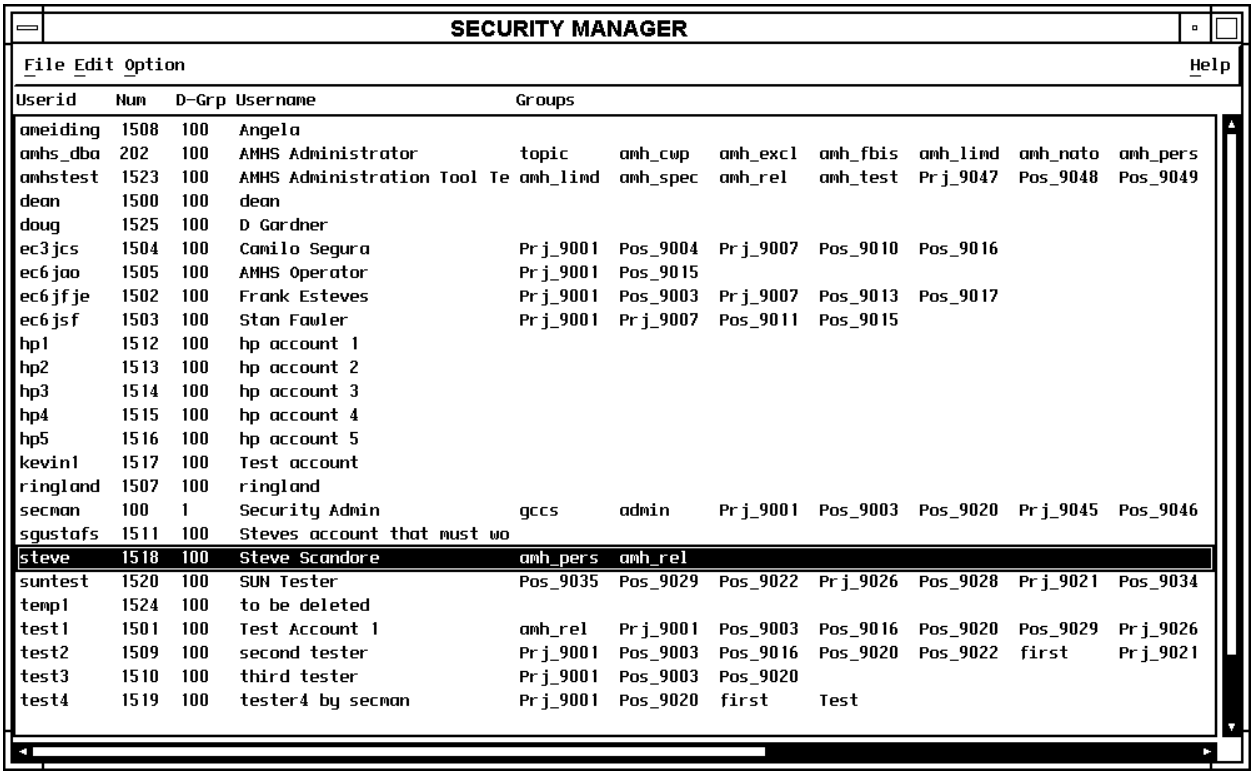
The Security Administrator has the responsibility to assign user passwords, create new network accounts, modify existing accounts, delete existing accounts, and view various audit logs and lists of special access category AMHS messages (limited distribution [LIMDIS], exclusive, etc.). Release is not considered a special access category but rather a privilege. The Security Administrator can accomplish these functions through the use of Security Manager audit log and root access to a UNIX Xterm.

The Security Manager desktop session is an interactive program that allows the Administrator to perform the various security administration functions through a set of capabilities built into the menu structure of these programs. The following paragraphs provide the necessary step-by-step actions required on your part to utilize the capabilities provided by the Security Manager computer program.

C.1.1 Security Manager Activation

To activate the Security Manager computer program, click twice in rapid succession on the SECURITY icon on the Session Manager's Launch Window while using the secman login (not just any login will do). Upon successful program initialization the Security Manager main window is displayed as shown in Figure C-1.

Note that for each account in the main window, there is a “USERID”, “Username" and "Group".



Userid	Num	D-Grp	Username	Groups						
ameiding	1508	100	Angela							
amhs_dba	202	100	AMHS Administrator	topic	amh_cwp	amh_excl	amh_fbis	amh_limd	amh_nato	amh_pers
amhstest	1523	100	AMHS Administration Tool Te	amh_limd	amh_spec	amh_rel	amh_test	Prj_9047	Pos_9048	Pos_9049
dean	1500	100	dean							
doug	1525	100	D Gardner							
ec3jcs	1504	100	Camilo Segura	Prj_9001	Pos_9004	Prj_9007	Pos_9010	Pos_9016		
ec6jao	1505	100	AMHS Operator	Prj_9001	Pos_9015					
ec6jfje	1502	100	Frank Esteves	Prj_9001	Pos_9003	Prj_9007	Pos_9013	Pos_9017		
ec6jsf	1503	100	Stan Fawler	Prj_9001	Prj_9007	Pos_9011	Pos_9015			
hp1	1512	100	hp account 1							
hp2	1513	100	hp account 2							
hp3	1514	100	hp account 3							
hp4	1515	100	hp account 4							
hp5	1516	100	hp account 5							
kevin1	1517	100	Test account							
ringland	1507	100	ringland							
secman	100	1	Security Admin	gccs	admin	Prj_9001	Pos_9003	Pos_9020	Prj_9045	Pos_9046
sgustafs	1511	100	Steves account that must wo							
steve	1518	100	Steve Scandore	amh_pers	amh_rel					
suntest	1520	100	SUN Tester	Pos_9035	Pos_9029	Pos_9022	Prj_9026	Pos_9028	Prj_9021	Pos_9034
temp1	1524	100	to be deleted							
test1	1501	100	Test Account 1	amh_rel	Prj_9001	Pos_9003	Pos_9016	Pos_9020	Pos_9029	Prj_9026
test2	1509	100	second tester	Prj_9001	Pos_9003	Pos_9016	Pos_9020	Pos_9022	first	Prj_9021
test3	1510	100	third tester	Prj_9001	Pos_9003	Pos_9020				
test4	1519	100	tester4 by secman	Prj_9001	Pos_9020	first	Test			

Figure C-1. Security Manager Main Window

C.1.2 Creating A New Account

(1) Click on **File -> Create Account** on the Security Manager menu bar. The Security Manager:Create Account Window is displayed. Note the default password is valid only for 24 hours. It is strongly recommended that you inform the user about this time limitation on the initial password.

(2) Type in all the text fields, including the SYBASE System Administrator Account Password. The Password is not visible as you type it in.

(3) Click on the special access categories that this user will have, then click on **OK/Apply**. The new user account is added to the main window, in alphabetical order, with all the special access categories assigned to it.

(4) The newly created account is available for logon right away on the user workstations.

(a) Log into the EM Server as one of the System Administrator accounts. Although some accounts may have the security manager icon, only the System Administrator accounts have the privileges to create accounts for the user workstations.

(b) Create the new account using the Security Manager program. This will add the new user to the Solaris password files, create the new user's home directory, and update NIS+ credentials.

C.1.3 Delete An Account

(1) Run Security Manager by double-clicking its icon.

(2) Click on an account to be deleted from the main window. The selected account is highlighted.

(3) Click on **File -> Delete Account** on the Security Manager menu bar. The Security Manager: Delete Account window is displayed.

(4) Type in the SYBASE System Administrator account password. The password is not visible as you type it in.

(5) Click on **YES** or **NO** for the Delete User Directories and Files question.

(6) Click on **OK/Apply**. The selected account is deleted from the main window. The duration of the delete process may vary according to the answer in Step (4) above.

C.1.4 Setting DB Audit Parameters

This capability allows you, as the System Manager or the Security Manager, to set the operating parameters for the GCCS database audit daemon. The setting of parameters entails selecting a user, a table, and the operation(s) to be audited on the selected GCCS database tables.

(1) Click on **File -> DB Audit Parameters** on the Security Manager menu bar. The Security Manager:DB Audit Parameters window is displayed. Note the window contains a list of all the GCCS database (DB) table names for which you can select audit operations.

(2) Click on the user name for which you want to set the audit parameters. The name of the selected user will be highlighted.

(3) Click on the table name for which you want to set the audit parameters. The name of the selected table will be highlighted.

(4) Click on any combination of operations, Retrieve, Update, Insert, Delete in the Security Manager:DB Audit Parameters window.

(5) Click on **Auditing Off** in the Security Manager:DB Audit Parameters window. The button label changes to Auditing On. This is a must step if auditing of database operations is desired.

(6) Click on **Add Object**, or **Delete Object**, or **Delete All** in the Security Manager:DB Audit Parameters window, as appropriate.

(7) Click on **Reset** in the Security Manager:DB Audit Parameters window if you want to cancel all the selections you made in Steps (2) through (5).

(8) Click on **OK/Apply** in the Security Manager:DB Audit Parameters window. All the selection you made in Steps (2) through (6) are saved and an audit trail will be available to view through **Option -> Database Audit Reports** on the Security Manager menu bar.

C.1.5 Host Access Parameters

This capability is used to configure remote workstation access through the internet services provided by a specified host workstation. For example, the system can be configured to limit FTP access to a certain workstation.

(1) Click on **File->Host Access Parameters** on the Security Manager menu bar. This brings up the dialog window used to edit host access parameters.

(2) Use the File pull-down to open an access file. Access files are stored for each workstation on the network.

(3) Once the access file is opened, a list of internet services will be displayed in the service window along with a list of hostnames that are allowed access through the corresponding internet service.

(4) To configure an internet service, click on the internet service. In this case, ftpd.

(5) Once the service is selected, a Host Access List and a Hosts Available list are displayed. Simply click on a host from one list to move it to the other list. Hosts in the Host Access List will be allowed access through the selected internet service, while hosts left in the Hosts Available list will not be allowed.

(6) Once the changes are made, click on **File->Save Access File** to save the changes in an updated access file.

C.1.6 Updating Security Caveats

This capability allows you, as the System Administrator or the Security Manager, to update the security caveats list by adding new or deleting existing Security caveats.

(1) Click on **File -> Update Security Caveats** on the Security Manager menu bar. The Security Manager:Edit Caveats window is displayed.

(a) For Adding a Caveat

1) Type in the name of the new caveat in the Caveat Name text area in the bottom of the Security Manager:Edit Caveats window.

2) Click on **Add** in the Security Manager:Edit Caveats window. The new caveat name is added to the existing list.

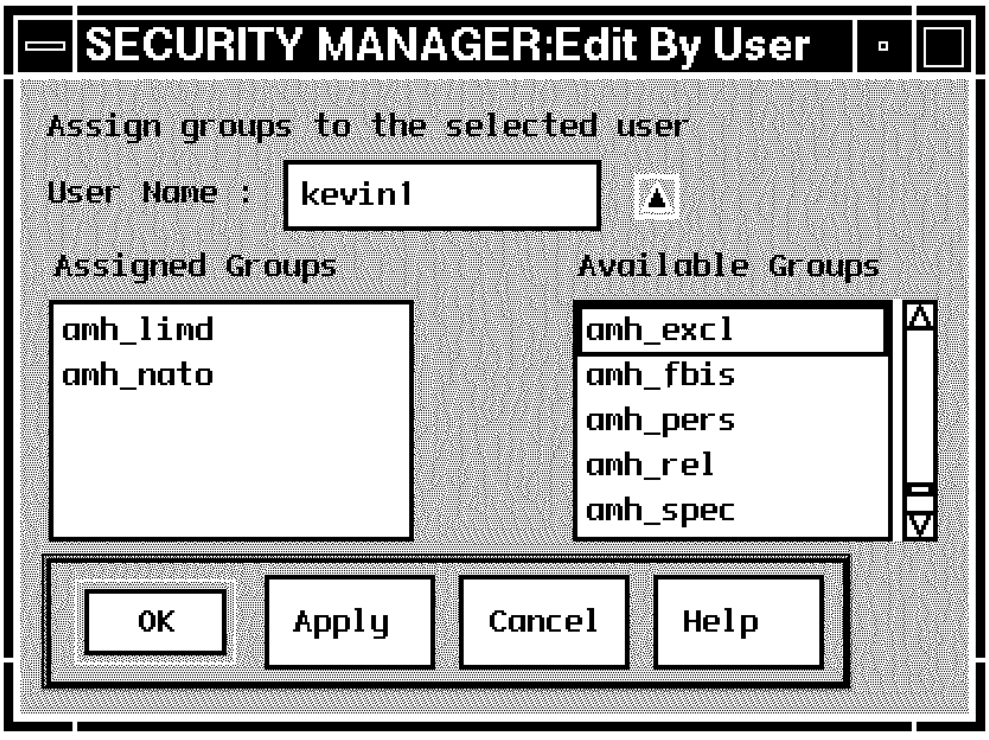
(b) For Deleting a Caveat

1) Click on the name of the caveat, in the existing list, that you want to delete. The selected name is highlighted and it appears in the Caveat Name text area in the bottom of the Security Manager:Edit Caveats window.

2) Click on **Delete** in the Security Manager:Edit Caveats window. The selected caveat name disappears from the existing caveats list.

C.1.7 Group Manipulations

This capability allows you, as the System Administrator or the Security Manager, to update the group list by adding, changing or deleting existing groups.



C.1.7.1 Creating A New Group

(1) Click on **File -> Groups -> New**. The New Groups window is displayed

(2) Enter the group name and group ID for the new group. The group ID should be unique to the new group. Read the UNIX “group” manual page for additional information about valid UNIX group IDs.

(3) Click on **OK** to add the group.

C.1.7.2 Changing A Group

(1) Click on **File -> Groups -> Change**. The Change Groups window appears.

(2) Select the group to change in the first entry field and type in the new group name in the second entry field

(3) Click on **OK** button to effect the change.

C.1.7.3 Deleting A Group

(1) Click on **File -> Groups -> Delete**. The Delete Groups window appears.

(2) Select the group to delete and click on **OK** to delete the group.

C.1.7.4 Edit User's Groups

(1) Click on **File -> Groups -> Edit** User's Groups. The Edit User's Groups window appears.

(2) Select the user from among the list of users.

(3) Two listings will be displayed:

(a) Groups to which the user belongs, and

(b) Groups to which the user doesn't belong.

Click on a group to move it from on listing to the other. Click **OK** to finish editing.

C.1.8 Obtaining Audit Reports

(1) System Audit Reports.

Allows you, with default to the last 24 hours (DTG Zulu), to display a UNIX system log for each of the following (one at a time): All Logins, Failed Logins, Privileged Commands, and Unauthorized Access. To obtain an UNIX audit report display do the following:

(a) Click on **Option -> System Audit Reports** on the Security Manager menu bar. The Security Manager:UNIX Audit Reports window is displayed. Note the period of audit is the last 24 hours.

(b) Click on the type of audit log you want to be displayed by clicking on one of the following options:

1) All Logins (default).
2) Failed Logins.
3) Privileged Commands.
4) Unauthorized Access.

(c) Set the correct audit period and Hostname and the click on Display in the Security Manager:UNIX Audit Reports window. The selected audit log type in Step (2) is displayed.

(d) Repeat Steps (2) and (3) for each audit log type.

(e) To obtain a printout of the report, click on the Print button at the bottom of the window and follow the direction provided.

(2) Database Audit Reports.

Allows you, with default to the last 24 hours (DTG Zulu), to obtain a Database audit report. The report contains the date, event, user name and pass/fail indication for the event. To obtain a database audit report do the following:

(a) Click on **Option -> Database Audit Reports** on the Security Manager menu bar. The Security Manager:Database Audit Reports window is displayed. Note the period of audit is the last 24 hours.

(b) Set the correct audit period and click on **Display** in the Security Manager:Database Audit Reports window. The report containing the audit trail is displayed.

(c) Click on **Print** in the Security Manager:Database Audit Reports window if you want a printout of the database audit report.

C.1.9 Security Manager Pull-Down Menus

The Security Manager has the following pull-down menus: File, Edit, View, Option and Help, which are shown in Figure C-2.

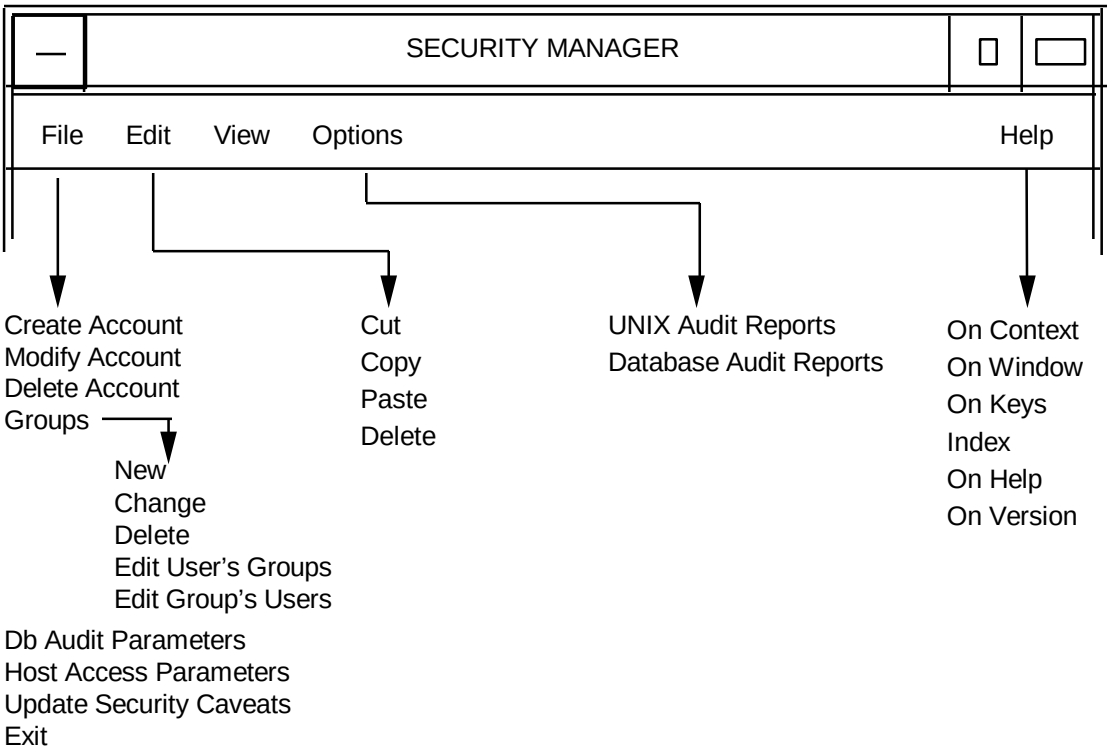


Figure C-2. Security Manager Pull-Down Menus

C.1.9.1 File Pull-Down

(1) Create Account. This selection allows you to create and add a new user account to the GCCS system.

(2) Modify Account. This selection allows you to modify an existing account.

(3) Delete Account. This selection allows you to delete an existing account with or without its associated directories and files.

(4) DB Audit Parameters. This selection allows you to select database audit parameters such as Operations, Logins and Logoffs.

(5) Host Access Parameters. This selection is used to configure remote access security through
the internet services (e.g., rlogin, FTP, etc.).

(6) Update Security Caveats. This selection allows you to add and/or delete caveats to/from an existing list.

(7) Exit. Allows you to exit the computer program, however you must first confirm the Exit request via a confirmation window.

C.1.9.2 Edit Pull-Down

Cut, Copy, Paste and Delete using standard editing tools.

C.1.9.3 View Pull-Down

On the EM Server, in the Security Manager main window, all users are displayed with their privileges and group memberships.

C.1.9.4 Option Pull-Down

(1) Solaris Audit Reports. This allows you, with default to the last 24 hours, to display a UNIX system log for each of the following (one at a time): All Logins, Failed Logins, Privileged Commands, and Unauthorized Access.

(2) Database Audit Reports. This allows you, with default to the last 24 hours, to display the GCCS Database log.

C.2 PROFILE MANAGER

The Profile Manager desktop session is an interactive program that is used to manage user profile information such as the creation, modification, and deletion of project and position information. The following paragraphs provide the necessary step-by-step actions required on your part to utilize the capabilities provided by the Profile Manager computer program.

To activate the Profile Manager computer program, double-click on the **PROFILE** icon on the Session Manager's Launch Window. Upon successful program initialization, the Profile Manager main window is displayed as shown in Figure C-3. This window contains two distinct areas: the top portion of the window, which is where selected profiles are displayed, and the bottom portion of the window, which is used as a filter.

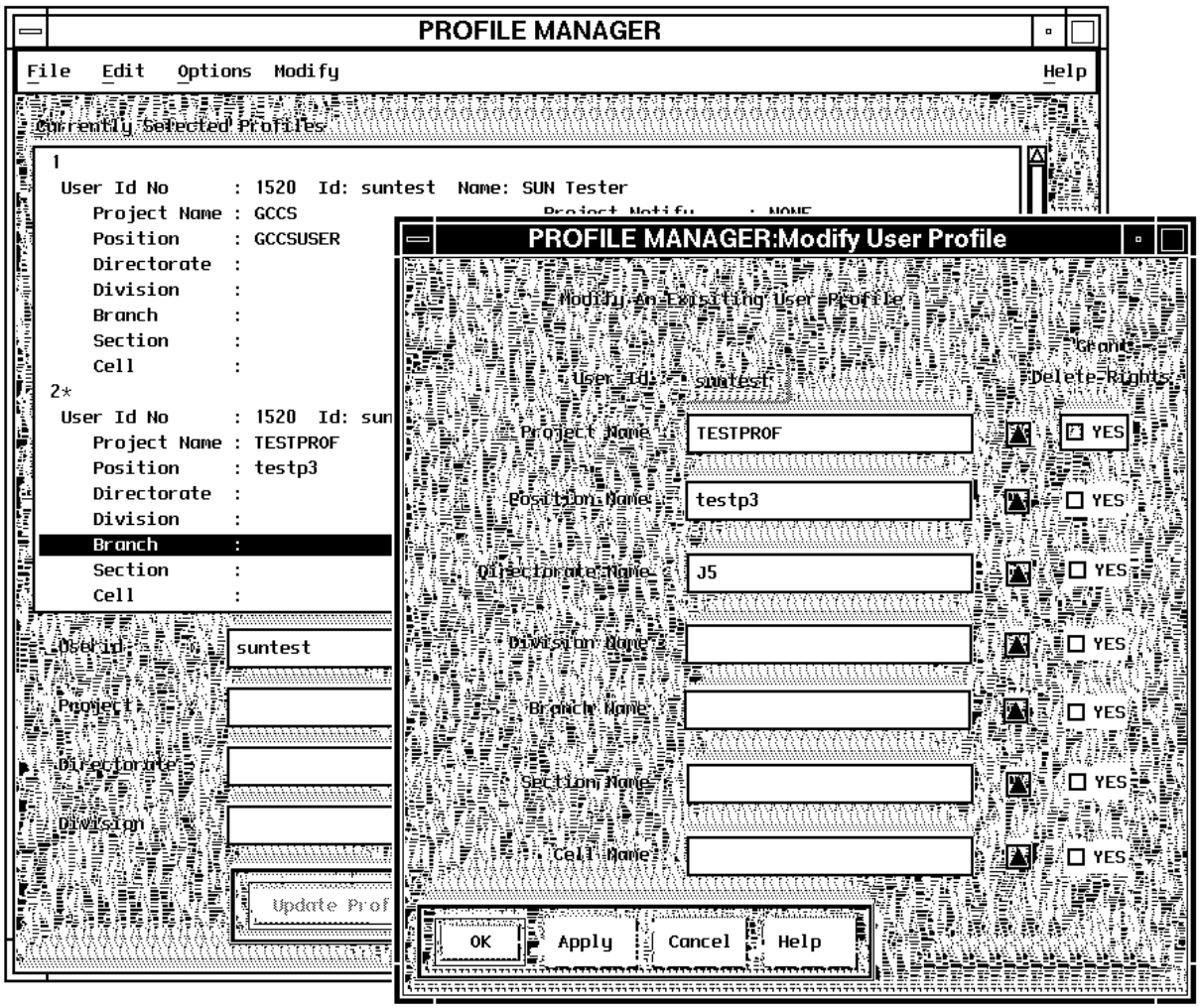


Figure C-3. Profile Manager Main Window

C.2.1 Filtering Profiles

As explained in the previous paragraph, the Profile(s) displayed in the main window can be filtered according to criteria listed in the bottom of the main window. Each filter criterion is selected from a popup selection list. To display Profile(s) that correspond to a certain filter criteria, do the following:

(1) Click on a popup selection button for a filter criterion to change the order in which the profiles are displayed. The popup selection dialog for the selected filter criterion is displayed.

(a) Click on the name of the selection you want to use for this filter criterion.

(b) Click on **OK/Apply**. The selected name appears in the corresponding filter criterion text field in the main window. If at this point you want to change your selection, click on Undo in the popup selection dialog. Your last selection is removed from the main window. Note that the Update Profile Filter and Clear Profile Filter buttons at the bottom of the main window become active after the first filter criterion is entered (these buttons are initially stippled).

(2) Repeat Step (1) above for each filter criterion you are interested in.

(3) Click on **Update Profile Filter** button on the main window. All user Profiles that meet the filter criteria are displayed in the main window with the default profile being marked by an asterisk (*). Also included on this display are the organization Notify and Delete Rights indicators. When the Notify indicator displays NOTIFY, the user will be notified when messages are received for that organization. The Delete Rights indicator displays DELETE, indicating the user has been given Delete Rights to elements in that organization's folder.

(4) Click on **Clear Profile Filter** to erase all filter criteria previously selected, and the Profiles displayed in the main window. This action results in the Update Profile Filter and the Clear Profile Filter buttons becoming stippled again.

C.2.2 Creating A New Project

(1) Click on **File -> New -> Project** on the Profile Manager menu bar. The Add a New Project dialog is displayed.

(2) Type in the name of the new project (maximum of 25 characters; no special characters are allowed). If you want the Default Positions list to be used with this new project, click on the Use Default Positions button in the Add a New Project dialog. If you want to create or edit the default position list, use the procedure outlined in Paragraph C.2.3.

(3) Click on **OK/Apply** to save the new project name.

C.2.3 Creating A New Position

(1) Click on **File -> New -> Position** on the Profile Manager menu bar. The Add a New Position dialog is displayed.

(2) Since all positions belong to a project, select a Project Name via the popup selection button.

(3) Type in the name of the new position (maximum of 8 characters; no special characters are allowed).

(4) Type in the description of the Position Name (maximum of 25 characters).

(5) Click on **OK/Apply** to save the new position name.

(6) Repeat Steps (1) through (5) for every new position you want to create.

C.2.4 Creating A New Directorate

(1) Click on **File -> New -> Directorate** on the Profile Manager menu bar. The Add a New Directorate dialog is displayed.

(2) Type in the name of the new Directorate (maximum of 25 characters).

(3) Click on **OK/Apply** to save the new Directorate name.

C.2.5 Creating A New Division

(1) Click on **File -> New -> Division** on the Profile Manager menu bar. The Add a New Division dialog is displayed.

(2) Type in the name of the new Division (maximum of 25 characters).

(3) Click on **OK/Apply** to save the new Division name.

C.2.6 Creating A New Branch

(1) Click on **File -> New -> Branch** on the Profile Manager menu bar. The Add a New Branch dialog is displayed.

(2) Type in the name of the new Branch (maximum of 25 characters).

(3) Click on **OK/Apply** to save the new Branch name.

C.2.7 Creating A New Section

(1) Click on **File -> New -> Section** on the Profile Manager menu bar. The Add a New Section dialog is displayed.

(2) Type in the name of the new Section (maximum of 25 characters).

(3) Click on **OK/Apply** to save the new Section name.

C.2.8 Creating A New Cell

(1) Click on **File -> New -> Cell** on the Profile Manager menu bar. The Add a New Cell dialog is displayed.

(2) Since all cells belong to a project, select a Project Name via the popup selection button.

(3) Type in the name of the new Cell (maximum of 25 characters).

(4) Click on **OK/Apply** to save the new Cell name.

C.2.9 Creating A New User Profile

(1) Click on **File -> New -> User Profile** on the Profile Manager menu bar. The Add a New User Profile window is displayed. Note that every entry into this window is done via a popup selection dialog and that Delete Rights can be set for each entry. The mandatory entries are User ID, Project Name, and Position Name. Additionally, before you can select a Position Name and/or a Cell Name, you must select a Project Name.

(a) Click on the popup selection dialog buttons for those fields that you want to become part of the User Profile.

(b) Select the **Grant Delete Rights** button if the user will have the right to delete folders and folder elements contained in the selected organization's folder. The user is granted delete rights if the Grant Delete Rights button is pushed in (button shaded).

(2) Click on **OK/Apply**. Your entries are verified, and if they are valid, the new User Profile you just created is added into the system.

C.2.10 Deleting A Project

(1) Click on **File -> Delete -> Project** on the Profile Manager menu bar. The Delete an Existing Project dialog is displayed. Note the warning that all profiles assigned to this project will be deleted.

(2) Select the Project to be deleted via the popup selection button.

(3) Click on **OK/Apply** to delete the selected project name.

C.2.11 Deleting A Position

(1) Click on **File -> Delete -> Position** on the Profile Manager menu bar. The Delete an Existing Position dialog is displayed.

(2) Select a Project Name via the popup selection button.

(3) Select a Position Name via the popup selection button.

(4) Click on **OK/Apply** to delete the selected position name.

C.2.12 Deleting A Directorate

(1) Click on **File -> Delete -> Directorate** on the Profile Manager menu bar. The Delete an Existing Directorate dialog is displayed. Note the warning that all profiles assigned to this Directorate will be deleted.

(2) Select a Directorate Name via the popup selection button.

(3) Click on **OK/Apply** to delete the selected Directorate name.

C.2.13 Deleting A Division

(1) Click on **File -> Delete -> Division** on the Profile Manager menu bar. The Delete an Existing Division dialog is displayed. Note the warning that all profiles assigned to this Division will be deleted.

(2) Select a Division name via the popup selection button.

(3) Click on **OK/Apply** to delete the selected Division name.

C.2.14 Deleting A Branch

(1) Click on **File -> Delete -> Branch** on the Profile Manager menu bar. The Delete an Existing Branch dialog is displayed. Note the warning that all profiles assigned to this Branch will be deleted.

(2) Select a Branch name via the popup selection button.

(3) Click on **OK/Apply** to delete the selected Branch name.

C.2.15 Deleting A Section

(1) Click on File -> Delete -> Section on the Profile Manager menu bar. The Delete an Existing Section dialog is displayed. Note the warning that all profiles assigned to this Section will be deleted.

(2) Select a Section name via the popup selection button.

(3) Click on **OK/Apply** to delete the selected Section name.

C.2.16 Deleting A Cell

(1) Click on **File -> Delete -> Cell** on the Profile Manager menu bar. The Delete an Existing Cell dialog is displayed.

(2) Select a Project name via the popup selection button.

(3) Select a Cell name via the popup selection button.

(4) Click on **OK/Apply** to delete the selected Cell name.

C.2.17 Delete A User Profile

(1) With the profile you want to delete displayed in the main window, click anywhere within this profile.

(2) Click on **File -> Delete -> User Profile** on the Profile Manager menu bar. The Delete User Profile window is displayed containing the profile you selected for deletion.

(3) Click on **OK/Apply**. The selected profile is deleted and is not recoverable.

C.2.18 Cut, Paste, Copy And Delete Capabilities

Cut, Copy and Delete selections must be preceded by a selection of text to be placed in a clipboard, upon which the Cut and Paste or Copy and Paste or Delete operations are to be performed.

(1) Select Text. You can select text by dragging the mouse from the first character through the last displayed character to be selected. The selected text appears in reverse video.

(2) Cut. Cut and Paste actions relocate text from one area to another. After selecting text, select **Edit -> Cut** which places the text in the clipboard. Please note that the selected text has disappeared. (The Copy function, discussed below, should be used if you want to retain the original text.)

(3) Copy. Copy and Paste activities result in replication of an existing text string.

(a) Select the text to be copied. The selected text appears in reverse video.

(b) Select **Edit -> Copy**. This places the text in the clipboard.

(4) Paste. Immediately after a Cut or Copy, pasting should be performed.

(a) Click the mouse at the exact location where you wish to paste the text from the clipboard.

(b) Select **Edit -> Paste**. The text that you have just cut or copied appears in the cursor location.

(5) Delete. After selecting text as described in Step (1) above, click on **Edit -> Delete** on the Profile Manager menu bar. The selected text is deleted and the space is compressed.

C.2.19 Profiles Display Order

Once profiles are displayed in the Currently Displayed Profiles area of the main window, you have the capability to change the order in which they are displayed. The default ordering is by User ID. Profiles can be ordered (in alphabetical order) according to the following criteria:

(1) User ID.
(2) Project.
(3) Position.
(4) Directorate.
(5) Division.
(6) Branch.
(7) Section.
(8) Cell.

To order the Profiles listed according to a specific criteria:

(9) Click on **Options -> Order By -> <a criteria>,** where <a criteria> is one of the eight criteria listed in (1) through (8) above. After a short time, the Currently Selected Profiles display in the main window is updated to reflect the order according to the criterion that you have selected. The ordering priority is as follows:

(a) Blanks.
(b) Numbers.
(c) UPPER CASE LETTERS.
(d) lower case letters.

C.2.20 Modifying A Project

(1) Click on **Modify -> Project** on the Profile Manager menu bar. The Modify Existing Project dialog is displayed.

(2) Select the Project name to be modified via the popup selection button.

(3) Type in the new Project name (maximum of 25 characters; no special characters are allowed).

(3) Click on **OK/Apply** to modify the selected Project name.

C.2.21 Modifying A Position

Position modification entails the following: modifying the name of a position within a project, modifying the list of Launch Buttons assigned to a position, and modifying the default list of positions assigned to a new project.

(1) To modify a position name within a project:

(a) Click on **Modify -> Position -> Name** on the Profile Manager menu bar. The Modify an Existing Position dialog is displayed.

(b) Select the Project name via the popup selection button.

(c) Select the old Position name via the popup selection button.

(d) Type in the new Position name (maximum 8 characters; no special characters are allowed).

(e) Click on **OK/Apply** to modify the selected old Position name.

(2) To modify a position Launch Button list:

(a) Click on **Modify -> Position -> Launch List** on the Profile Manager menu bar. The Edit Position Launch List dialog is displayed.

(b) Select the Position name via the popup selection button. The list of all available Launch Buttons is displayed in the right side of the Edit Position Launch List dialog. On the left side are all the Launch Buttons that are currently assigned to the selected position. Click on a name in one list to move it to the other.

(c) Click on **OK** to save the assigned Launch Button list.

(3) To modify a position Default List:

(a) Click on **Modify -> Position -> Default List** on the Profile Manager menu bar. The Edit Default Position List dialog is displayed. The list of commonly used Positions is displayed in the right side of the Edit Default Position List dialog. On the left side are all the default positions. Click on a name in one list to move it to the other.

(b) Click on **OK/Apply** to modify the Default List.

C.2.22 Modifying A Directorate

(1) Click on **Modify -> Directorate** on the Profile Manager menu bar. The Modify Existing Directorate dialog is displayed.

(2) Select an old Directorate name via the popup selection button.

(3) Type in the new Directorate name (maximum of 25 characters).

(4) Click on **OK/Apply** to modify the selected Directorate name.

C.2.23 Modifying A Division

(1) Click on **Modify -> Division** on the Profile Manager menu bar. The Modify Existing Division dialog is displayed.

(2) Select an old Division name via the popup selection button.

(3) Type in the new Division name (maximum of 25 characters).

(4) Click on **OK/Apply** to modify the selected Division name.

C.2.24 Modifying A Branch

(1) Click on **Modify -> Branch** on the Profile Manager menu bar. The Modify Existing Branch dialog is displayed.

(2) Select an old Branch name via the popup selection button.

(3) Type in the new Branch name (maximum of 25 characters).

(4) Click on **OK/Apply** to modify the selected Branch name.

C.2.25 Modifying A Section

(1) Click on **Modify -> Section** on the Profile Manager menu bar. The Modify Existing Section dialog is displayed.

(2) Select an old Section name via the popup selection button.

(3) Type in the new Section name (maximum of 25 characters).

(4) Click on **OK/Apply** to modify the selected Section name.

C.2.26 Modifying A Cell

(1) Click on **Modify -> Cell** on the Profile Manager menu bar. The Modify an Existing Cell dialog is displayed.

(2) Select a Project name via the popup selection button.

(3) Select an old Cell name via the popup selection button.

(4) Type in the new Cell name (maximum of 25 characters).

(5) Click on **OK/Apply** to modify the selected Cell name.

C.2.27 Modifying A User Profile

(1) With the profile you want to modify displayed in the main window, click anywhere within this profile.

(2) Click on **Modify -> User -> Profile** on the Profile Manager menu bar. The Modify an Existing User Profile window is displayed containing the profile you selected for modification. All entries, except User ID, can be modified via popup selection buttons.

(3) Make all the modifications you want.

(4) Click on **OK/Apply**. The selected profile is modified per your selections in Step (3).

C.2.28 Modifying A User Launch List

(1) Click on **Modify -> User -> Launch List** on the Profile Manager menu bar. The Edit User Launch List window is displayed.

(2) Select a **User ID** via the popup selection button. All launch buttons available are listed in the right side of the Edit User Launch List. The left side contains the launch buttons that are assigned to the User ID selected. Click on a right side name to move it to the left side, or click on the left side to move it to the right side.

(3) Click on **OK** to save a user launch list.

C.2.29 Profile Manager Pull-Down Menus

The Profile Manager has five pull-down menus: File, Edit, Options, Modify, and Help. These pull-downs are shown in Figure C-4.

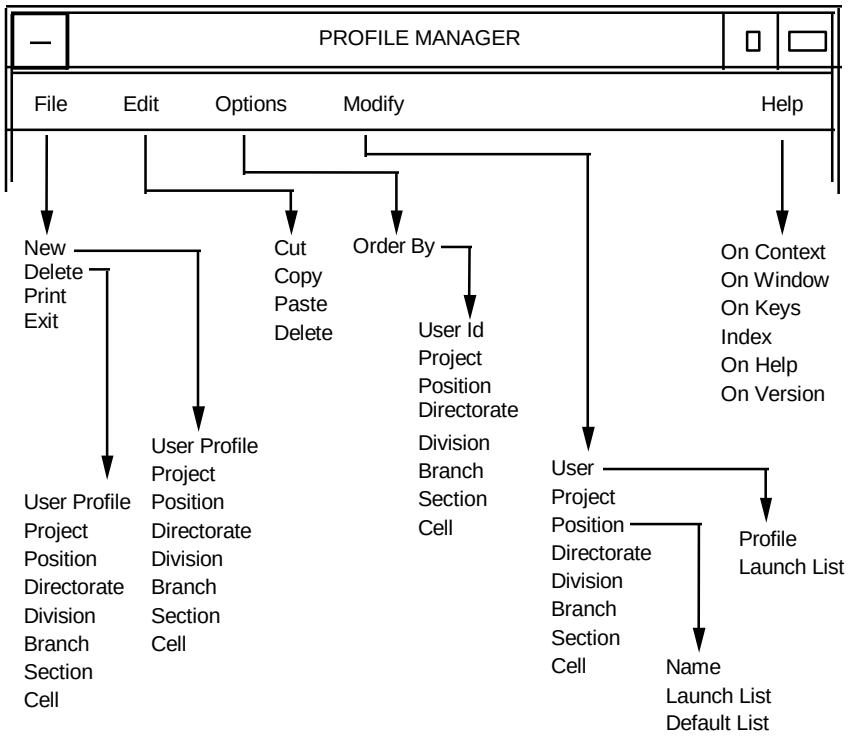


Figure C-4. Profile Manager Pull-Down Menus

C.2.29.1 File Pull-Down

(1) New. Allows you to add new entries into the system.

(2) Delete. Allows you to delete entries from the system.

(3) Print. This selection allows you to print complete user profiles from the Profile Manager's main window display area.

(4) Exit. Allows you to exit the computer program; however, you must first confirm the Exit request via a confirmation window.

C.2.29.2 Options Pull-Down Menu

The Options pull-down menu selection Order By allows you to display the content of the Profile Display window in an order based on one of a set of choices. Initially all profiles are sorted by User ID.

C.2.29.3 Modify Pull-Down Menu

(1) User. Allows you to modify a user's Profile or Launch List.

(2) Project. Allows you to modify the name of an existing Project.

(3) Position. Allows you to:

(a) Change a Position name within a specified Project.

(b) Assign a list of Launch Buttons to a Position. These are displayed in the Session Manager window.

(c) Assign a default list of Positions to subsequently created Projects.

(4) Directorate. Allows you to modify the name of an existing Directorate.

(5) Division. Allows you to modify the name of an existing Division.

(6) Branch. Allows you to modify the name of an existing Branch.

(7) Section. Allows you to modify the name of an existing Section.

(8) Cell. Allows you to modify the name of an existing Cell within a specified Project.

C.3 SYSTEM MONITOR

System Monitor desktop session provides the System Operator with the capability to monitor system resources, review and print system logs, and send/receive system alarms. To activate the System Monitor computer program, double-click on the MONITOR icon on the Session Manager's Launch Window. Upon successful program initialization, the System Monitor main window is displayed as shown in Figure C-5.

C.3.1 Obtaining Status Information from the Main Window

The main window contains the names and status of all the processors/workstations currently connected to the GCCS. As seen in the figure, the top portion of the main window displays the status of the critical GCCS servers, while the bottom portion displays the status of the workstations. This window is updated as information changes and becomes available.

(1) Processors. The status of each processor can be UP, DEGR, or DOWN. The status appears to the right of the processor name in the processor information window after clicking and highlighting one of the workstations listed in the System Maintenance window.

(2) Workstations. The status of each workstation can be UP, DEGR, or DOWN. Whatever the status is, it appears on the right side on the bottom of the main window. To obtain detailed information on any workstation:

(a) Click on the line corresponding to the workstation for which you want to obtain detailed status information. The System Monitor:Processor Information window is displayed. This window is updated as information changes and becomes available.

1) Processor Name.
2) Description of the processor function.
3) Current user ID.
4) Last internal comm message received by the workstation.
5) Percent CPU utilization.
6) Memory utilization (in kilobytes).
7) List of processes being monitored.

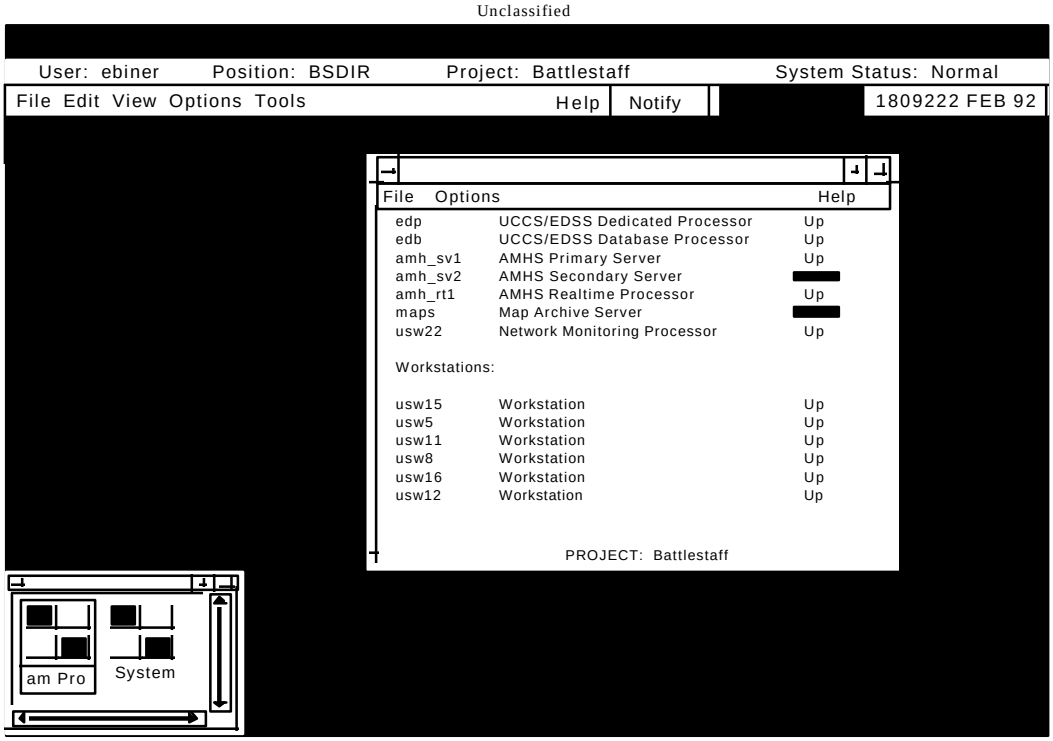


Figure C-5. System Monitor Main Window

(b) Click on the **Help** button on the bottom of the window to obtain Help on the processor information window.

(c) Click on the **Close** button on the bottom of the window to close the processor information window.

C.3.2 Printing Capabilities

(1) Main Window. To print the main window, click on **File -> Print** on the System Monitor menu bar.

(2) Processor Information. To print the information regarding the processors connected to the GCCS, click on the status button representing the processor whose information you want to print out. Upon the display of the Processor Information window, click on the Print button within the window.

(3) Logs. To print the current System Log and/or any archived system log, do the following:

(a) Click on **Options -> Log Reporter -> System Log** (or any archived system log) on the System Monitor menu bar. The Log Reporter window is displayed.

(b) Click on Filters and select the criteria for generating the log and then click on Create. The log based on the filter criteria selected is displayed.

(c) Click on **Print** on the bottom of the Log Reporter window.

(4) Incoming System Alarm. To print the Incoming System Alarm log, do the following:

(a) Click on **Options -> Display Incoming Alarms** on the System Monitor menu bar. The Incoming System Alarm window is displayed.

(b) Click on **Print** on the bottom of the window.

NOTE: Printing will clear the alarm queue.

C.3.3 Displaying Current Users

This selection presents you with a current list of all GCCS users logged into the GCCS workstations. For each user, the User's ID, Position, Hostname, and assigned user name is given.

(1) Click on **Options -> Current Users Display** on the System Monitor menu bar. The System Monitor:Current Users window is displayed.

(2) Click on **Close** to close the window and get back to the main window.

C.3.4 Displaying Log Information

This selection presents you with the system log (current), and with up to ten archived system logs.

(1) Click on **Options -> Log Reporter -> System Log** (or any archived system log) on the System Monitor menu bar. The Log Reporter window is displayed.

(2) Click on **Filters** and select the criteria for generating the log and then click on Create. The log based on the filter criteria selected is displayed.

(3) Click on **Next Page/Previous Page** until you find the log entry you want to display.

C.3.5 Generating System Alarms

This selection allows you to generate and send system messages to all running Session Managers.

(1) Click on **Options -> Generate System Alarm**. The System Monitor:Send System Alarm dialog containing a scrollable text entry field is displayed.

(2) Click on the Clear button to clear the text, if any, in the text field.

(3) Type in the text of the system-wide message you want to send.

(4) Click on the **Send** button. You will hear a string of short beeps (if beeping is enabled through Preferences). These beeps come from the Session Manager notifying you that a message has arrived. The Session Manager:System Alarm window containing the message you have sent is displayed on all Session Manager workstations.

(5) Click on **Cancel** in the Session Manager Alarm window to close it.

(6) Click on **Close** in the System Monitor pull-down Alarm window to close it.

C.3.6 Incoming System Alarms

The System Monitor computer program has the capability to receive system alarms from the GCCS system executive software. Any message that is classified Serious or Fatal is sent to the GCCS system executive is forwarded to the System Monitor computer program. These messages will appear in an Incoming System Alarm window. Incoming messages are stored in a 100 message queue as they are received. After the limit is reached, the oldest message is replaced by the newest message. To display the incoming alarms, do the following:

(1) Click on **Options -> Display Incoming Alarms** on the System Monitor menu bar. The Incoming System Alarm window is displayed.

(2) Click on the **Next** or **Prev** buttons on the Incoming System Alarm window to scan through the message queue. Note the Number of Entries counter on the top right corner of the incoming alarm dialog; it displays the current message number followed by the total number of messages in the queue.

(3) If you want the Incoming System Alarm window to be displayed automatically upon receipt of an alarm, set the Automanage button to On. Otherwise, the Incoming System Alarm log will be displayed only upon specifically requesting it through Options -> Display Incoming Alarms on the System Monitor menu bar.

C.3.7 Viewing UNIX Files

As a System Operator, you may have the capabilities (through an Xterm window) to create a list of UNIX files that you can later review via a pull-down menu. After the list of files has been created, do the following to view any file in the list:

(1) Click on **Option -> File Viewer** on the System Monitor menu bar. A dialog window containing the list of files that you can view is displayed.

(2) Click on the file you want to view. The file you selected is highlighted.

(3) Click on **OK/Apply**. The selected file is displayed. You can scroll up/down in the file to view its contents.

C.3.8 UNIX Tools

There are a wide variety of system status reporting tools that the operator may use to monitor system operations and diagnose system problems. This section provides a brief description of the most useful status reporting mechanisms. For detailed information about each of the commands described herein, issue the following UNIX command:

man *command* <return>

where ***command*** is any one of the following commands.

Command	Description
iostat	Displays a report of current I/O statistics
ps	Displays a report of system process status, use **ps -eaf** to see the status of all running processes.
uptime	Displays a report of how long the system has been up.
vmstat	Displays a report of virtual memory statistics.
rwho	Displays a report of all users logged on to any computer in the network.
netstat	Displays network activity.
nfsstat	Displays activity on the NFS.
df -k	Display mounted filesystems and disk usage.

C.3.9 System Monitor Pull-Down Menus

The System Monitor has three pull-down menus: File, Options, and Help which are shown in Figure C-6.

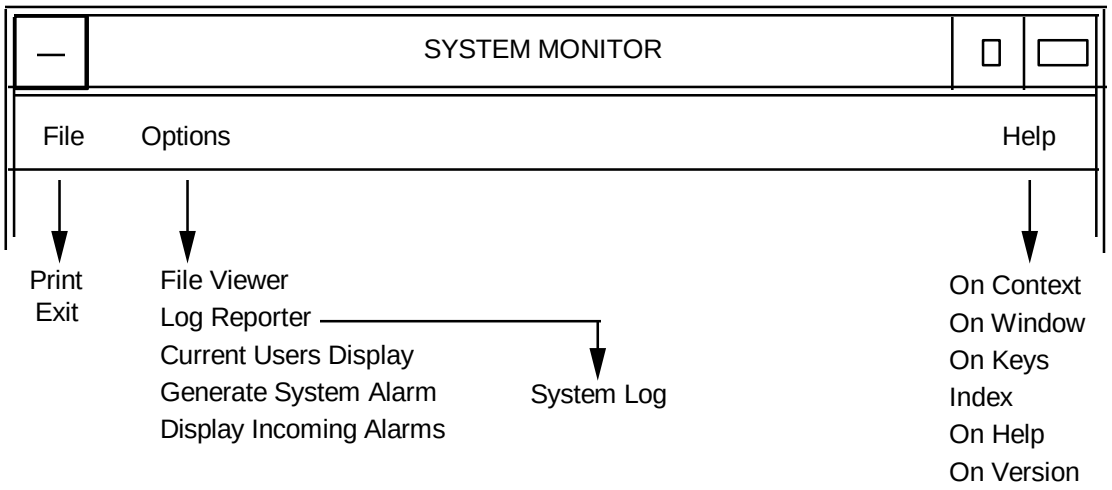


Figure C-6. System Monitor Pull-Down Menus

C.3.9.1 File Pull-Down

(1) Print. This selection allows you to obtain printouts of the main System Monitor computer program window.

(2) Exit. Allows you to exit the computer program, however you must first confirm the Exit request via a confirmation window.

C.3.9.2 Options Pull-Down

(1) File Viewer. This selection allows you to read and re-read repeatedly UNIX files via a pull-down menu.

(2) Log Reporter. This selection presents you with the System Log and up to ten archived system logs designated by the date-time-group (DTG) of the actual archive. A filter which is selectable by you is also available.

(3) Current Users Display. This selection presents you with a current list of all GCCS users logged into the GCCS. For each user, the User's ID, Position, Hostname and assigned user name is given.

(4) Generate System Alarms. This selection allows you to generate and send system messages to all running Session Managers.

(5) Display Incoming Alarms. This selection allows you to display all incoming system alarms currently in the System Alarm queue.

C.4 SYSTEM CONTROLLER

The System Controller computer program is an interactive program that permits the System Administrator on one GCCS workstation to manage processes on other GCCS workstations on the LAN. The System Controller function is available to you only if the System Controller icon is displayed in your launch window.

The System Controller function provides you, the System Administrator, the capability to manage and control resources at workstations other than the one where you are working. This remote control is accomplished by using the GCCS Local Executive (LE) at your workstation to send System Controller commands to its counterpart on the destination workstation, with commands forwarded through the GCCS System Executive (SE). The list of System Controller commands is maintained in a configuration file which you can edit. A sample excerpt from the System Controller configuration file is provided in Figure C-7. The LE on the destination workstation will then return any information and status to the LE on the requesting workstation using the SE as the forwarder. This interaction between the various workstation local executives and the SE is illustrated in Figure C-8.

The following paragraphs provide the necessary step-by-step actions required on your part to utilize the capabilities provided by the System Controller computer program. To activate the System Controller function, double-click on the System Controller icon in the Session Manager launch window. The System Controller main window will be displayed as illustrated in Figure C-9.

```
# Control Command Table
#
# This file is used to map system control directives
# to unix executables. Each system control type will
# begin in the first column. Make sure that the control
# types do not have any extra spaces at the end of the
# line, and that the control names are in uppercase.
#
# All lookup names must be indented and immediately
# follow the corresponding command directive. The
# absence of an indented line that follows a command
# directive marks the end of the lookup names in the
# respective command directive.
#
##############################################################################
#
# STARTUP:
#   Each entry in the startup control type requires
#   four fields: the service name, user description,
#   executable name, and user. The third field
#   is used to specify the process real and effective
#   user id. Each field is separated by a semicolon.
#
STARTUP
   u5mapdmn;Map Daemon Utility;root;/usr/edss/bin/map_daemon
   u5rltexc;Activity Scheduler;root;/usr/edss/edp/mac_start /usr/users/edp/activity_scheduler
   u5audsrv;Database Audit;root;/usr/edss/edp/mac_start /usr/edss/edp/ude_audit
   edsstma;Tma Application;root;/usr/edss/bin/tma_main

##############################################################################
#
# SHUTDOWN:
#   Each entry in the shutdown control type requires
#   four fields: the service name, user description,
#   executable uid, and executable command.
#
SHUTDOWN
   u5sysexc;System Executive;root;/usr/edss/bin/mac_control_send shutdown u5sysexc
   u5rltexc;Activity Scheduler;root;/usr/edss/bin/mac_control_send shutdown u5rltexc
   u5audsrv;Database Audit;root;/usr/edss/bin/mac_control_send shutdown u5audsrv

##############################################################################
#
# INIT:
#   This control types requires two three fields:
#   the service name, user description, and
#   executable command to perform the init.
#   An init is used to cause certain service
#   programs to reexecute their initialization
#   routines.
#
INIT
   u5sysexc;Gccs System Executive;/usr/edss/bin/mac_control_send init u5sysexc
   u5rltexc;Activity Scheduler;/usr/edss/bin/mac_control_send init u5rltexc
   u5audsrv;Database Audit;/usr/edss/bin/mac_control_send init u5audsrv
   u5mapdmn;Map Daemon Utility;/usr/edss/bin/mac_control_send init u5mapdmn
```

Figure C-7. Sample System Controller Configuration File

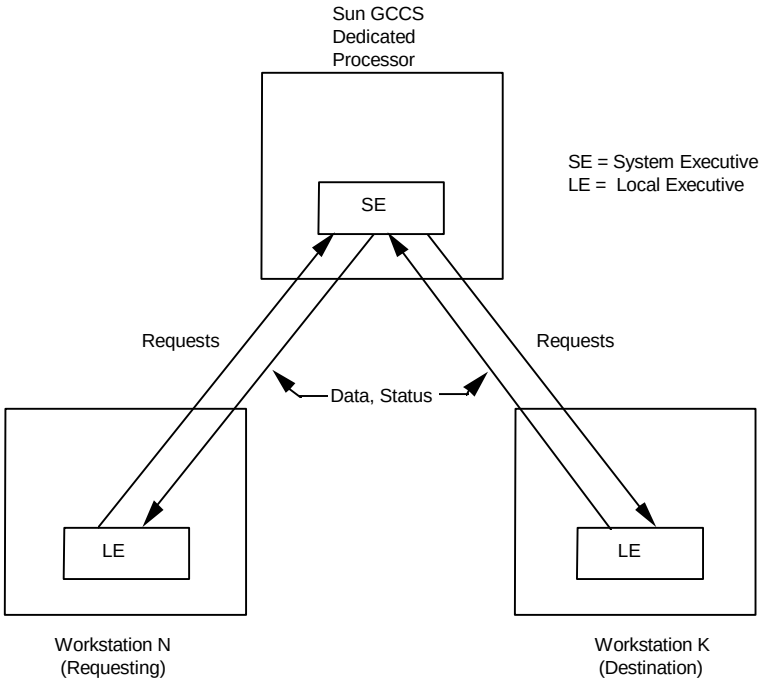


Figure C-8. System Controller Interaction Between LEs and the SE

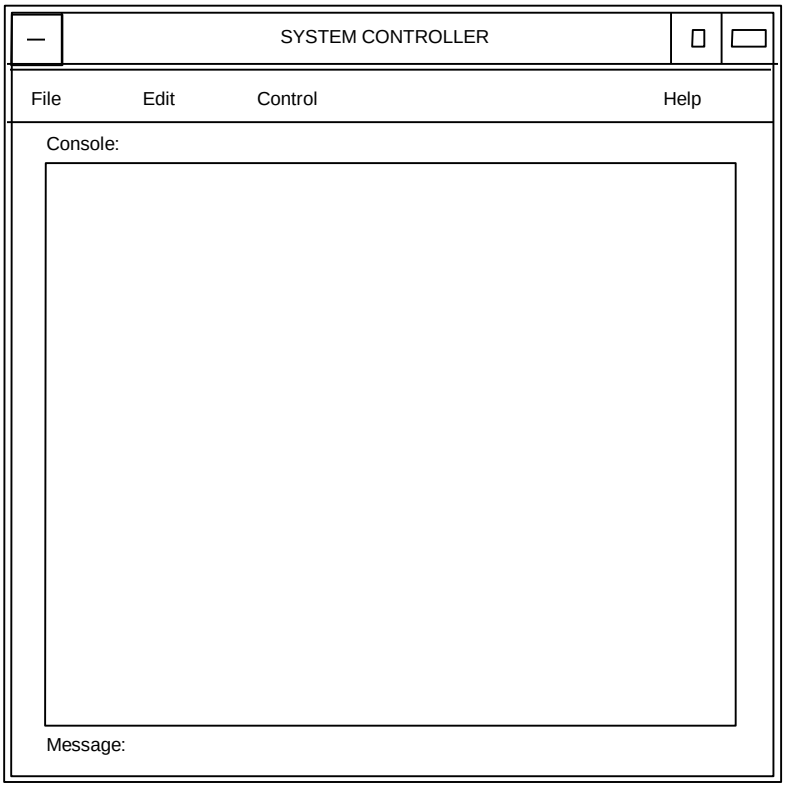


Figure C-9. System Controller Main Window

C.4.1 Starting Up Processes

(1) Click on **Control -> Startup** from the System Controller menu bar. A System Controller: Startup window is displayed as shown in Figure C-10.

(2) Click on the desired host name to select the host on which you want to start up a specific process (processes names are listed under the Servers column).

(3) Click on the desired process description to select the process to be started.

(4) Click on **OK** or **Apply** to send the appropriate startup command to the specified host. The wait cursor will appear until a status is returned from the GSE. The status is then displayed in the message area at the bottom of the System Controller main window. Any errors encountered during startup are displayed in an error dialog box.

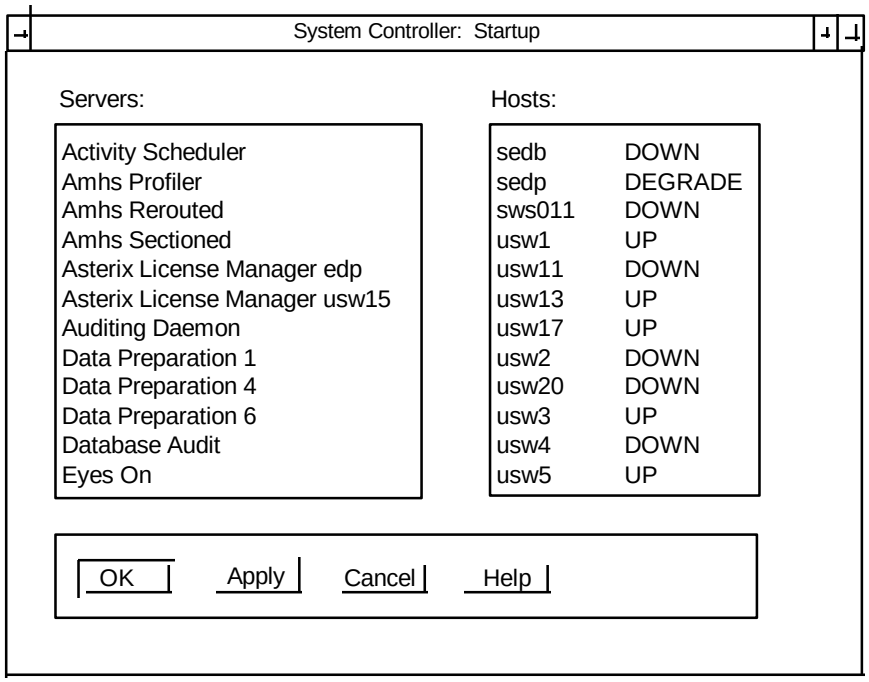


Figure C-10. System Controller Startup Window

C.4.2 Shutting Down Processes

(1) Click on **Control -> Shutdown** from the System Controller menu bar. A System Controller: Shutdown window is displayed.

(2) Click on the desired host name to select the host on which you want to shut down a specific process.

(3) Click on the desired process description to select the process to be shut down.

(4) Click on **OK** or **Apply** to send the appropriate shutdown command to the specified host. The wait cursor will appear until the shutdown status is returned from the GSE. The status is then displayed in the message area at the bottom of the System Controller main window. Any errors encountered during this shutdown are displayed in an error dialog box.

C.4.3 Killing Processes

(1) Click on **Control -> Kill** from the System Controller menu bar. A System Controller: Kill window is displayed as shown in Figure C-11.

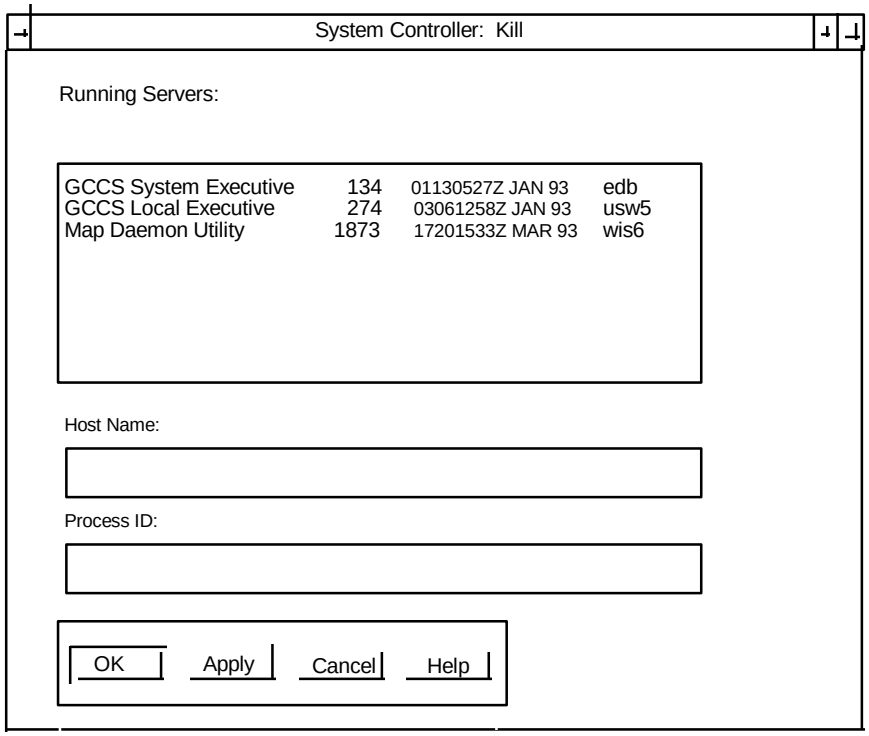


Figure C-11. System Controller Kill Window

(2) Click on the process to be killed from the list of Running Servers. The selection is highlighted. If the process to be killed is not registered or is not displayed, enter the host name and process ID in the windows provided.

(3) Click on **OK** or **Apply** to send the appropriate kill command to the specified host. The wait cursor will appear until a status is returned from the GSE. The status is then displayed in the message area at the bottom of the System Controller main window. Any errors encountered are displayed in an error dialog box.

C.4.4 Initializing Processes on Remote Workstations

(1) Click on **Control -> Initialize** from the System Controller menu bar. A System Controller: Initialize window is displayed, as shown in Figure C-12, listing all of the currently active processes that have registered their process ID (PID), host name, and process start time.

(2) Click on the currently active process that you want to go through its initialization process again. The selection is highlighted.

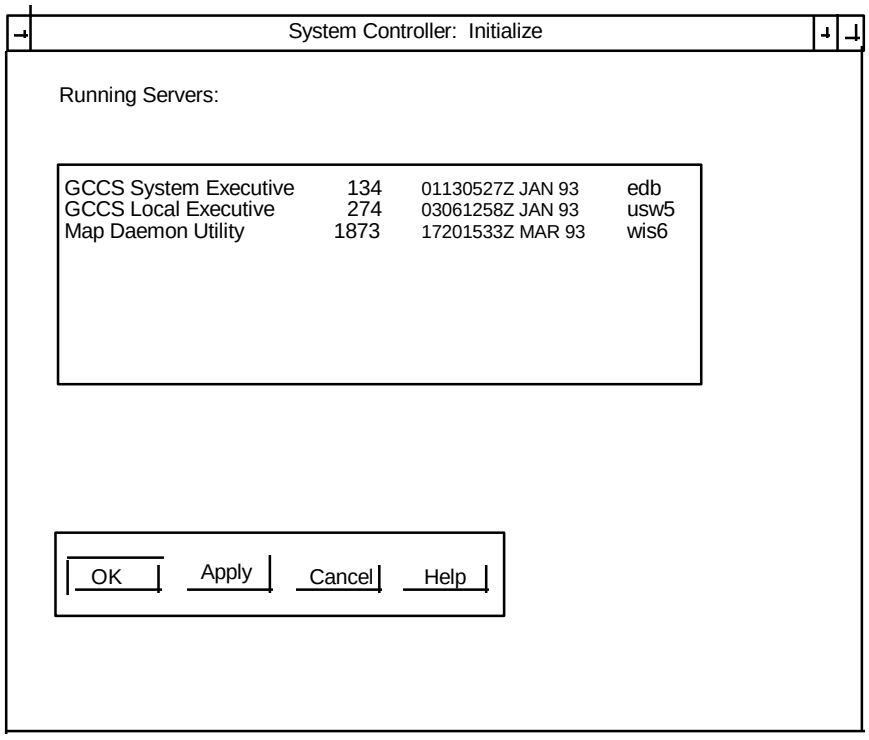


Figure C-12. System Controller Initialize Window

(3) Click on **OK** or **Apply** to send the appropriate initialize request to the specified host. The wait cursor will appear until a status is returned from the GSE. The status of the initialization is then displayed in the message area at the bottom of the System Controller main window. Any errors are displayed in an error dialog box.

C.4.5 Executing Commands on a Remote Workstation

(1) Click on **Control -> Execute** from the System Controller menu bar. A System Controller: Execute window is displayed as shown in Figure C-13.

(2) In the Host window, click on the name of the desired host on which the command is to be executed.

(3) In the Command window, type in the desired UNIX command. Multiple UNIX commands can be chained together by typing a semicolon (;) between them.

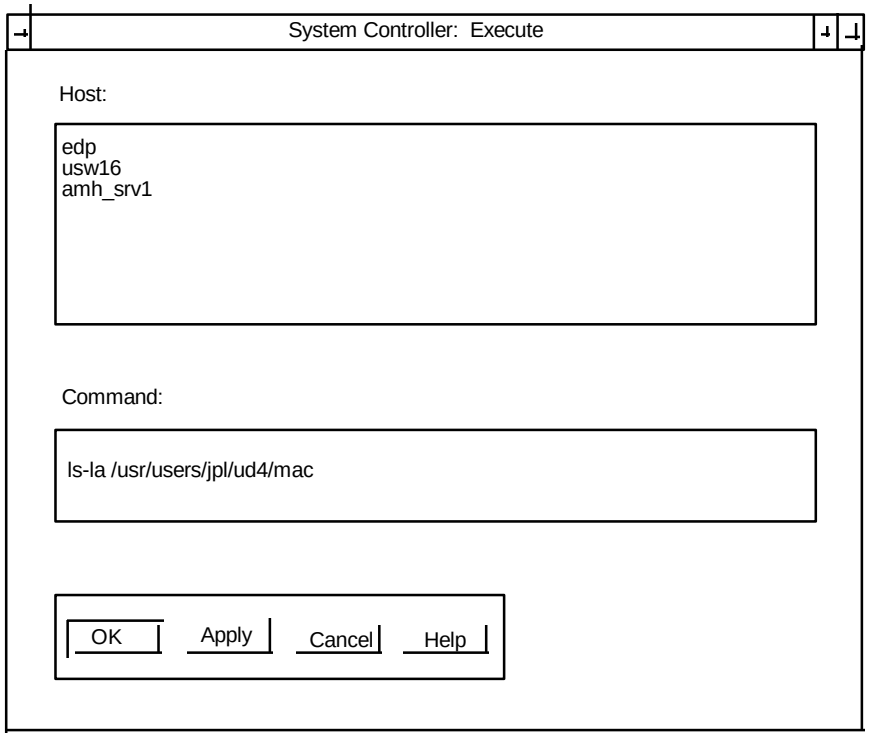


Figure C-13. System Controller Execute Window

(4) Click on **OK** or **Apply** to send the specified command(s) to the selected host. The wait cursor will appear until a status is returned from the GSE. The status of the commands is then displayed in the message area at the bottom of the System Controller main window. The output from the commands is displayed in the main window. If the command takes awhile to execute, the additional output will appear every five (5) seconds.

C.4.6 Displaying and Printing A Report

To display a predefined system monitor report for any remote host, do the following:

(1) Click on **Control -> Report** from the System Controller menu bar. A System Controller: Report window is displayed as illustrated in Figure C-14.

(2) Enter/select the name of the desired host on which the report is about.

(3) In the Report window, click on the report that you want to display. The selected report name is highlighted.

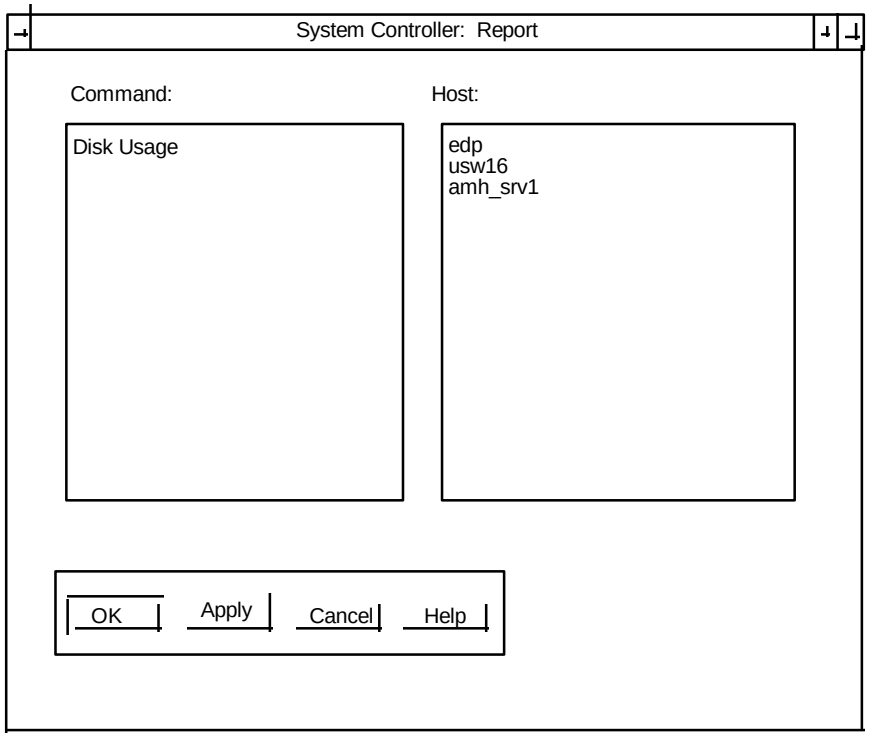


Figure C-14. System Controller Report Window

(4) Click on **OK** or **Apply** to issue the commands that generate and display the requested report. The wait cursor will appear until the report is displayed at your workstation. Any errors are displayed in an error dialog box. The output from the command is displayed in the main window. If the report takes awhile to generate and be displayed, the additional output will appear every five (5) seconds.

(5) Click on **File -> Print** on the System Controller menu bar to print the displayed report.

C.4.7 System Controller Pull-Down Menus

The System Controller has four pull-down menus: File, Edit, Control and Help. These pull-downs are shown in Figure C-15 and described below.

C.4.8 File Pull-Down

(1) Print. This selection allows you to print the text output or console text window in the System Controller display area.

(2) Exit. Allows you to exit the computer program. However, you must first confirm the Exit request via a confirmation window.

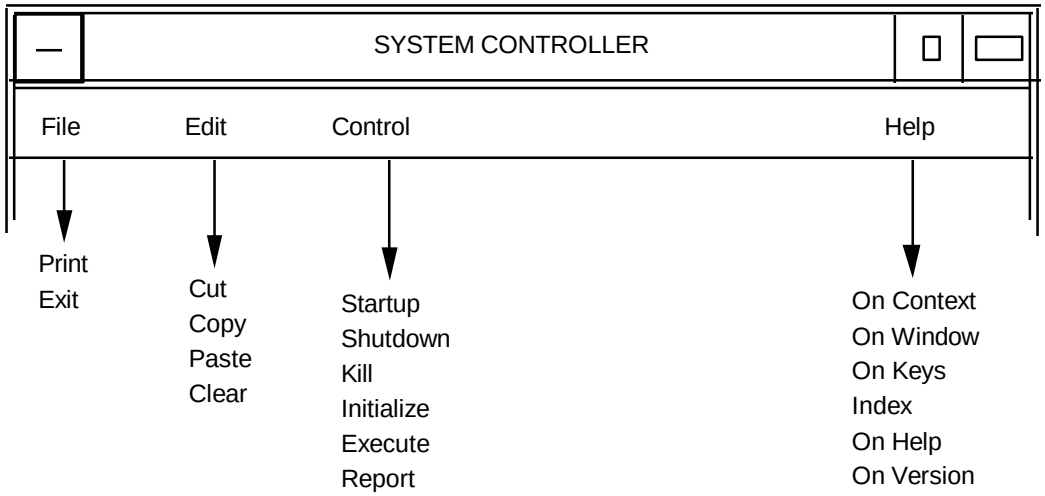


Figure C-15. System Controller Pull-Down Menus

C.4.9 Control Pull-Down Menu

(1) Startup. This selection allows you to select processes on other GCCS workstations to be started from your workstation. The processes are selected from a predefined System Controller configuration file.

(2) Shutdown. This selection allows you to gracefully terminate processes on designated GCCS workstations. The processes that can be shut down are defined in the System Controller configuration file. Each specified process will close any open files and perform an orderly termination.

(3) Kill. This selection allows you to stop (i.e., kill) a registered process on a specified GCCS workstation.

NOTE: This selection may result in the loss of data which was not saved to the database or to disk.

(4) Initialize. This selection tells a registered application on a designated GCCS workstation to reinitialize itself.

(5) Execute. This selection allows you to issue a command to be executed at another GCCS workstation.

(6) Report. This selection allows you to select a System Monitor report from a predefined list to be generated for display. A report on disk usage or memory utilization are examples of reports which can be requested for display.

NOTE: A registered GCCS process is one which has provided its process ID and process name to the Monitor and Control function and is one of those processes identified to be controlled by the System Controller function.

C.5 SYBASE ADMINISTRATION

This section provides the description of various tasks performed by the GCCS System Administrator and Database Administrator (DBA). Some of the tasks are performed according to certain SOPs that have been developed. Some of the other tasks are performed using the SYBASE Stored Procedures (SPs) (sp_xxxx, where xxxx is the SP name). Section C-5 contains several important Sybase maintenance SOPs.

These procedures are typical and must be adapted to site-specific SOPs.

C.5.1 SYBASE Checks

The DBA has the responsibility to verify that SYBASE processes are running. To verify that the processes are indeed running, perform the following:

(1) Login to SUDB as **root**. (SUDB is the hostname of the Sybase Server)

(2) Type: **ps -eaf | grep sybase <RETURN>**.

There should be at least one SYBASE process running. The process **/dataserver** should be running for the GCCS SYBASE server.

(3) If the server is not running, it needs to be restarted. To do that perform the following:

(a) Type: **cd /h/COTS/SYBASE/install <RETURN>**.

(b) Enter the name of the process to be restarted; e.g., **RUN_GCCS.**

(4) If the SQL processes are running but problems are encountered, SYBASE may need to be shut down and restarted. Some typical SYBASE problems are listed below:

(a) GSE cannot launch Position Log (PLOG).

(b) System is extremely slow.

(c) Errors and continuous time-outs occur when building slides and maps.

(5) To shut down SYBASE (only as a last resort), do the following:

(a) From the SUDB prompt, type:

cd /h/COTS/SYBASE <RETURN>.

(b) Type: **isql -Usa -GCCS <RETURN>**.

(c) Enter **<password> <RETURN>**.

(d) At the "1>" prompt, type: **shutdown <RETURN>**.

(e) At the "2>" prompt, type: **go <RETURN>**.

(f) The console should display the following message:

Server shutdown by request DB Library:
unexpected EOF by SQL server
SUDB:root<>

(6) To restart SYBASE, perform the following:

(a) Type: **cd /h/COTS/SYBASE <RETURN>**.

(b) Type: **RUN_GCCS <RETURN>**.

(c) Type: **showserver <RETURN>**. This will display the SYBASE processes,

(7) If Step (6) fails to restart SYBASE, then shut down the SUDB server and reboot the system per standard startup procedures..

C.5.2 Removing Old PLOG Entries

For system efficiency and better performance, it is advisable that PLOG entries older then a predetermined time be removed from the PLOG. To remove old entries perform the following:

(1) Login to SEDP as **root** (rlogin sedp -l root).

(2) Enter **<password> <RETURN>**.

(3) Type: **cd /h/EM/admin/admin_tools <RETURN>**.

(4) Type: **delete_old_plog_entries <RETURN>**.

(5) In response to the prompt "Please enter Sybase System Administrator account:" type: **sa <RETURN>**.

(6) In response to the prompt "Please enter Sybase System Administrator password:" type: **<password> <RETURN>**.

(7) In response to the prompt "Please enter PLOG table to be archived:" type: **<name of position (in upper case)> <RETURN>**. Example: **CMDDIR**.

(8) In response to the prompt "Please enter number of PLOG entries to be retained:" type: **<number of PLOG entries to be kept> <RETURN>**.

(9) Some messages will be displayed on the screen to show that the program is running.

C.5.3 Stored Procedures

SPs are stored procedures that Structured Query Language (SQL) server supplies for use in the administration of the database. These procedures are provided as shortcuts for retrieving information from the system tables, or mechanisms for accomplishing database administration and other tasks that involve updating system tables. The list of the system procedures is a very long one. This section lists some of them in order to provide the Administrator with a top level view of these procedures. A complete list of all the system procedures can be found in the "SYBASE SQL Server, Release 10 - System Administration Guide".

C.5.3.1 Managing SQL Server Logins And Database Users

This section describes methods for managing SQL server login accounts and database users.

For more details, refer to the "SYBASE SQL Server, Release 10 - System Administration Guide," Chapter 4.

C.5.3.1.1 Adding New Users

The process of adding new users consists of the following steps:

(1) The DBA creates a login account for the user with the system procedure *sp_addlogin*

(2) The DBA adds the user to the database with the system procedure *sp_adduser*

The following is a summary of commands (in CAPS) and system procedures (in *italics*) used for adding new users:

Command/ Procedure	**Task**	**Permission**	**Where (DB)**
sp_addlogin	create new logins assign passwords assign default DBs	DB Administrator	master
sp_addgroup	create groups	DB Administrator	GCCS
sp_adduser	add users to DB assigns aliases assign groups	DB Administrator	GCCS
grant	grant groups or	DB Administrator users permission on commands and database objects	GCCS

The “permission” column specifies the lowest default permission level, while the "where" column specifies the database in which the *process*/**COMMAND** must be performed.

(1) Adding Users to SQL Server.

The system procedure *sp_addlogin* adds new login names to SQL Server. The syntax for this procedure, executable by the Database Administrator only, is as follows:

sp_addlogin loginame [, passwd [, default db]]

From the three parameters associated with this procedure, only the first one (loginame) is mandatory. The other two are optional. If a default database parameter is not specified, the default database is *master*. In order to discourage user from using the master database, always assign a default database to new users.

(2) Creating Groups.

Groups on SQL Server can be created at any time with the procedure *sp_addgroup.* The syntax for this procedure is as follows:

sp_addgroup grpname

For example, to set up the Senior Engineering group, issue this command:

sp_addgroup senioreng.

C.5.3.1.2 Adding Users To Databases

The procedure *sp_adduser* adds a user to the GCCS DB. The user must already be a SQL Server user, i.e., the DBA must have added the user to SQL Server with *sp_addlogin*. The syntax for *sp_adduser* is as follows:

sp_adduser loginame [, name_in_db [, grpname]]

The first parameter to *sp_adduser* is the login name of an existing user. This is the only required parameter. The other two are optional.

C.5.3.1.3 Dropping Logins, Users, And Groups

The following system procedures allow the Database Administrator to drop logins, users, and groups:

Procedure	Task	Permission	Where (DB)
sp_droplogin	drop user from	DBA	master
sp_dropuser	drop user from DB	DBA	GCCS
sp_dropgroup	drop group from DB	DBA	GCCS

(1) Dropping Logins.

The system procedure *sp_droplogin* denies a user access to SQL Server. The syntax for *sp_droplogin* is as follows:

sp_droplogin login_name.

(2) Dropping Users.

The system procedure *sp_dropuser* denies an SQL Server user access to the database in which it is executed. The syntax for dropping a user from the database is as follows:

sp_dropuser name_in_db

name_in_db is usually the login name. This procedure can only be executed by the DBA.

(3) Dropping Groups.

A group that has members cannot be dropped. If you attempt to remove a group with members, the error report will display a list of the members of the group you are attempting to drop. The syntax to drop a group is:

sp_dropgroup groupname.

C.5.3.1.4 Changing User Information

The following procedures allow you to change any of the user information that has been previously added.

Procedure	Task	Permission	Where (DB)
sp_password	change another user's password	DBA	
sp_changegroup	change group assignment of a user	DBA	GCCS
sp_modifylogin	change a login account's default database, or full name	DBA	GCCS

(1) Changing Password.

The syntax for changing any user's password is:

sp_password caller_password, new_password [, login_name]

where,

caller_password is the password of the login account currently executing sp_password.

new_password is the new password for the user executing sp_password, or for the user indicated by login_name.

(2) Changing Groups.

The syntax for changing groups is as follows:

sp_changegroup group_name, name_in_db

When a user changes from one group to another, the user looses all permissions that he/she had as a result of belonging to the old group. He/she gains all the permissions that have been granted to the new group.

(3) Changing User Defaults.

A user can change his/her default database, default language, or full name at any time by using the **sp_modifylogin** procedure. The syntax is as follows:

sp_modifylogin login_name, option, value

where,

login_name is the name of the user whose account you are modifying

option specifies the option that you are changing; e.g., **defdb**, **deflanguage**, **fullname**

value is the new value for the specified option.

C.5.3.1.5 Getting Information On Users

The following procedures allow users to obtain information about users, groups, and current SQL Server usage:

Procedure	Task
sp_who	reports on current SQL Server users and processes
sp_helpuser	report on users in a DB
sp_helpgroup	reports on groups within a DB

(1) Reports on Current Users and Processes.

The system procedure *sp_who* reports information on current users and processes on SQL Server. The syntax is as follows:

sp_who [loginame | "spid"].

The parameter loginame is optional. If it is specified, the report will contain information about the processes run by the specified user. If the loginame parameter is not specified, the procedure will report the processes run by all users. The following is an example of the results of running the *sp_who* procedure without a parameter:

spid	status	loginame	hostname	blk	dbname	cmd
1	runnable	dba	doc	0	master	SELECT
2	sleeping	dba		0	master	NET HNDLR
3	runnable	peter	kermit	0	pubs2	SELECT

(3 rows affected)

(2) Information on Users.

The system procedure *sp_helpuser* reports information on authorized users of the current database. Its syntax is as follows:

sp_helpuser [name_in_db]

The parameter "name_in_db" is optional. If it is specified, the report will contain information about that user. If the "name_in_db" parameter is not specified, the procedure will report on all users. The procedure reports the user's name in the database, the user ID, the user's login name, and the group name.

The following is an example of the results of running the *sp_helpuser* procedure without a parameter in a database called *pubs*:

users_name	id_in_db	group_name	login_name	default_db
dbo	1	public	dba	master
marcy	4	public	marcy	pubs
sandy	3	public	sandy	pubs
bob	7	senioreng	bob	master

(4 rows affected)

(3) Help on User Names and IDs.

To find a user's server User ID or login name, use the system functions *suser_id* and *suser_name*.

Function	Argument	Result
suser_id	(["server_user_name"])	server user ID
suser_name	([server_user_ID])	server user name (login name)

The arguments for these system functions are optional. If one is not specified, SQL Server displays information about the current user. For example:

```
select suser_name(3)
select suser_name( )
select suser_id("bob")
```

To find a user's ID number or name inside the database, use the system functions *user_id* and *user_name*.

Function	Argument	Result
user_id	(["db user name"])	user ID
user_name	([DB user ID])	user name

The arguments for these system functions are optional. If one is not specified, SQL Server displays information about the current user. For example:

```
select user_name(3)
select user_name( )
select user_id("ken")
```

C.5.4 Managing Physical Resources

C.5.4.1 Initializing Database Devices

A database device is dedicated to the storage of objects that make up databases. The term "device" does not necessarily refer to a distinct physical device. It can refer to any piece of disk (such as a partition) or a file in the file system that is used to store databases and database objects. Each database device must be prepared and made known to SQL Server before it can be used for database storage. This process is called *initialization.*

Once a database device is initialized, it can be:

(1) Allocated to the pool of space available to a user database.

(2) Allocated to a user database and assigned to store specific database objects.

(3) Used to store a database's transaction logs.

(4) Designated as a default device for **CREATE** and **ALTER DATABASE** commands.

New database devices are added by the DBA with the DISK INIT command whose syntax is as follows:

```
disk init
        name = "device_name" ,
        physname = "physicalname" ,
        vdevno = virtual_device_number ,
        size = number_of_blocks
        [, vstart = virtual_address ,
                cntrltype = controller_number ]
```

The NAME is the name of the database device.

The PHYSNAME is the name of a raw disk partition (UNIX) or the name of an operating system file.

VDEVNO is an identifying number for the database device. It is unique among devices used by SQL Server. Device number 0 is reserved for the device named *d_master*, that stores the system catalogs. Legal numbers are between 1 and 255 but cannot be greater than the number of database devices for which the system is configured. To determine the number to use for VDEVNO, the Database Administrator inspects the *device_number* column of the report from *helpdevice.*

The following query lists all the device numbers currently in use:

select distinct low/166777216 from sysdevices order by low

The SIZE of the database device is given in 2 kilobyte blocks. DISK INIT uses SIZE to compute the value for the high virtual page number in *sysdevices.high.*

VSTART is the starting virtual address, or the offset in 2 kilobyte blocks, for SQL Server to begin using the database device. The default value of VSTART is zero.

The optional CNTRLTYPE keyword specifies the disk controller. Its default value is zero.

For additional details, refer to the SYBASE SQL Server, Release10 -System Administration Guide, Chapter 3, under Initializing Database Devices.

C.5.4.1.1 Getting Information About Devices

When used without a device name, *helpdevice* lists all the devices available on SQL Server. When a device name is entered, it lists information about the device. In the following example, the shell command *sp_helpdevice* is used to report information on the *master* device:

sp_helpdevice master

Upon completing the execution of this procedure, the following information is displayed:

device_name:	**master**
physical_name:	**d_master**
description:	**special, default disk, physical disk, 20 MB**
status:	**3**
cntrltype:	**0**
device_number: **0**	
low:	**0**
high:	**9999**

For additional details, refer to the "SYBASE SQL Server, Release 10 - System Administration Guide," Chapter 3, under "Getting Information about Devices."

C.5.4.1.2 Dropping Devices

System procedure *sp_dropdevice* is used to drop databases and dump devices from *sysdevices.* The syntax is:

sp_dropdevice device_name

A device that is in use by a database cannot be dropped. The database must be dropped first.

WARNING: The SQL Server must be restarted after a device has been dropped because the kernel has a process that is accessing the dropped device. There is no other way to kill the process. Restarting frees up the virtual device number. The server is stopped with SHUTDOWN and restarted with *startserver* or *dataserver.*

For additional details, refer to the "SYBASE SQL Server, Release 10 - System Administration Guide," Chapter 3, under "Dropping Devices."

C.5.4.2 CREATE DATABASE Syntax

The CREATE DATABASE command can be issued only while using the Master Database. The CREATE DATABASE syntax is as follows:

```
create database database_name
        [on {default | database_device} [= size]
        [, database_device [= size]]...]
        [log on database_device [ = size ]]
        [, database_device [= size]]...]
        [with override]
        [for load]
```

For additional details, refer to the "SYBASE SQL Server, Release 10 - System Administration Guide," Chapter 3, under "Create Database Syntax."

(1) Database Size and Space Allocation

A new database can range in size from 2 megabytes to 2^{23} megabytes. If the amount of space requested on a specific database device is unavailable, SQL Server creates the database with as much space as possible on a per-device basis. It then displays a message stating how much space was actually allocated to each database device. (This is not considered an error.) The CREATE DATABASE command fails if there is less that the minimum space necessary for a database on the specified database device.

(2) Omitting the Size Parameter

If the size parameter in the ON clause is omitted, the database is created with the default amount of space.

If the size parameter in the LOG ON clause is omitted, the log device is allocated 2 megabytes of storage.

(3) Omitting the ON Clause

If the ON clause is omitted, the size of the database is the default size. The space is allocated from the default database device(s) indicated in *master..sysdevices*, in alphabetical order by database name.

(4) Omitting the LOG ON Clause

If the LOG ON clause is omitted, the database's transaction log is placed on the same database device as the data tables. Subsequent use of the system procedure *sp_logdevice* affects only future writes to the log and does not move the first few log pages that were written when the database was created. This leaves exposure problems in certain recovery situations and is not recommended.

C.5.4.3 DROP DATABASE Syntax

The DROP DATABASE command deletes the database and all of the objects in it from SQL Server, frees the allocated storage space, and deletes references to it from the system tables in the Master Database. The syntax for this command is:

drop database database_name [, database_name]...

As seen above, more than one database can be dropped in a single statement.

After a database is dropped, the master database should be dumped to ensure recovery in case *master* is damaged.

For additional details, refer to the “SYBASE SQL Server, Release 10 - System Administration Guide," Chapter 3, under "Drop Database Syntax."

C.5.4.4 ALTER DATABASE Syntax

The ALTER DATABASE command is used to increase the allocated space for a database if the initial allocation proves to be too small. Permission for this command defaults to the database owner and is automatically transferred with database ownership. The permission cannot be changed with the GRANT or REVOKE. The syntax for the ALTER DATABASE command is:

```
alter database database_name
        [on {default | database_device} [= size]
        [, database_device [= size]]...]
        [log on {default | database_device} [= size]
        [, database_device [= size]]...]
        [with override]
        [for load]
```

For additional details, refer to the "SYBASE SQL Server, Release10 - System Administration Guide," Chapter 3, under "Alter Database Syntax."

C.5.4.5 Information On Storage

To find the name(s) of the database device(s) on which a particular database resides, use the system procedure *sp_helpdb* with the database name:

sp_helpdb pubs

name	db_size	owner	dbid	created	status
pubs	3 MB	eb	6	Dec 7 1990	no options set

device_fragments	size	usage
pubsdev	2 MB	data only
tranlog	1 MB	log only

device	segment
pubsdev	default
pubsdev	system
tranlog	logsegment

When the *sp_helpdb* is used without arguments, it reports on all databases on SQL Server:

sp_helpdb

name	db_size	owner	dbid	created	status
master	**3 MB**	**eb**	**4**	**Dec 1 1990**	**no options set**
model	**2 MB**	**eb**	**3**	**Dec 1 1990**	**no options set**
pubs	**2 MB**	**eb**	**4**	**Nov 15 1988**	**no options set**
tempdb	**2 MB**	**eb**	**2**	**Jan 2 1991**	**select into /bulkcopy**

To get a summary on the amount of storage space used by a database, execute the system procedure *sp_spaceused:*

sp_spaceused

database_name	database_size	reserved	data	index_size	unused
pubs	**2 MB**	**832 KB**	**210 KB**	**52 KB**	**570 KB**

The procedure *sp_spaceused* can be used with an object name as its parameter, as follows:

sp_spaceused titles

name	rows	reserved	data	index_size	unused
titles	**18**	**48 KB**	**6 KB**	**4 KB**	**38 KB**

For additional details, refer to the "SYBASE SQL Server, Release10 - System Administration Guide," Chapter 3, under "Information on Storage."

C.5.5 Backup And Recovery

The SQL Server has automatic/non-automatic recovery procedures to protect you from power outages and computer failures. To protect yourself against media failure, you must make regular and frequent backups of your databases.

Automatic recovery is the process that protects the DBA from system failures. The automatic recovery mechanisms are run every time the SQL Server is restarted. Automatic recovery ensures that all transactions completed before a system crash are written out to the database device, and that all transactions not completed before a crash are removed.

The non-automatic recovery functions are accomplished using the DUMP and LOAD commands to load dumps from tapes or other dump media. The backups that the DBA makes with the DUMP DATABASE and DUMP TRANsaction commands are the only means to recover in case of a media failure.

Refer to the following documentation sources for detailed information related to the subject of backup and recovery:

For More Information About	See
dump, load, and **sp_volchanged** syntax	SYBASE SQL Server, Release10 - System Administration Guide, Chapter 8.
Backing up and restoring the system databases	SYBASE SQL Server, Release10 - System Administration Guide, Chapter 9.
Using thresholds to automate backups	SYBASE SQL Server, Release10 - System Administration Guide, Chapter 10.

DISTRIBUTION:

OSF
USARMY-OSF-DISA-JIEO
45335 Vintage Park Place
Sterling, VA 20166-6700
ATTN: MAJ T. Dorsey

USAISC
CMDR USAIS, ASWSD-IN
Geeley Hall
Ft. Huachuca, ZA 85613-5000
ATTN: Bob Griffiths

USAISMA
CCU/SPO
Squire Hall, Bldg. 283
ASQM-CCB
Ft. Monmouth, NJ 07703-5000
ATTN: Mr. John Minken

JPL
Atwood, S.
DeForrest, L.
Frey, W.
Roe, M.
Thomas, S.
Van Steenburg, R.